Paperless Everything: A Systematic Literature Review for the Design of Blockchain-based Document Management Systems

HAUKE PRECHT, Carl von Ossietzky Universität Oldenburg, Dept. Comp. Science, Germany
JOSCHKA ANDREAS HÜLLMANN, University of Twente, Department of Industrial Engineering and Business Information Systems, The Netherlands
JORGE MARX GÓMEZ, Carl von Ossietzky Universität Oldenburg, Dept. Comp. Science, Germany

Digitalization pushes organizations to increasingly rely on digital documents over physical documents. They offer unprecedented scalability and provide the foundation for fully digital processes. Despite their advantages, digital documents also have drawbacks compared to physical documents. Two key drawbacks are ownership transfer and document integrity. Blockchain technology can address these drawbacks. First, blockchain immutability characteristics enable tamper-proofing of digital documents. Second, consensus algorithms solve the "double-spending problem" for the ownership transfer of digital assets.

The technical feasibility of such blockchain-based document management systems has been prototyped in different domains. However, these studies focus on their respective domain only and do not communicate their insights back to the blockchain community. As a result, insights into the design and architecture of blockchain-based document management systems are scattered across domains. Best practices remain inaccessible to the blockchain community at large, impeding the gradual accumulation of knowledge and lasting impact.

This study reports on a systematic literature review of the architectural building blocks and patterns of blockchain-based document management systems. It is based on 1737 initially identified papers, of which 113 papers were analyzed in detail. The findings show that the commonly used architectures are proxy-based (48%) and dApp-based (38%), along with a favor for off-chain storage (68%). It is also shown that only 22% of papers mentioned best practices when it comes to testing and that the majority do not report implementation details. Based on the findings, this study recommends more rigorous justification and documentation of the architectural building blocks. Addressing concerns related to smart contract descriptions, storage, testing, and legal regulations such as the General Data Protection Regulation is encouraged, and future research opportunities for the design of blockchain-based document management systems are outlined to achieve impact in practice.

CCS Concepts: • **Applied computing** → **Document management**; • **Software and its engineering** → **Software architectures**; • **Computer systems organization** → *Distributed architectures*; • **General and reference** → Surveys and overviews.

Additional Key Words and Phrases: blockchain, document management system, blockchain-based document management system, architecture, best practices, literature review

Authors' addresses: Hauke Precht, hauke.precht@uol.de, Carl von Ossietzky Universität Oldenburg, Dept. Comp. Science, Ammerländer Heerstraße 114–118, Oldenburg, Lower Saxony, Germany, 26129; Joschka Andreas Hüllmann, j.huellmann@utwente.nl, University of Twente, Department of Industrial Engineering and Business Information Systems, Drienerlolaan 5, Enschede, The Netherlands; Jorge Marx Gómez, jorge.marx.gomez@uol.de, Carl von Ossietzky Universität Oldenburg, Dept. Comp. Science, Ammerländer Heerstraße 114–118, Oldenburg, Lower Saxony, Germany, 26129.

ACM 2769-6480/2025/6-ART
https://doi.org/10.1145/3737296

1 INTRODUCTION

The market for document management systems (DMSs) keeps growing rapidly, with estimates ranging from a market size of $23 to $67 billion and growth rates of 10-16% per year in 2023[1][2][3]. Key drivers for the growing markets are (a) the increased need to meet rising regulatory requirements, including confidentiality, verifiability, and authenticity of legal document trails, and (b) improved document and information governance in times of the information economy. The market grows across all industries, and new features are being developed, implemented, and rolled out, with cloud and decentralized technologies growing in popularity. Despite the market growth, paper-based documents remain commonly used for legal documents such as ownership, certificates, or contracts because electronic or digital documents can be easily forged [40, 52, 59].

The advent of distributed ledger technology (DLT) and blockchain technologies for DMSs promises tamper-proof record keeping along with the possibility to transfer ownership rights [167]. These features are critical to legal document management [16]. Prototypes of blockchain-based document systems have been developed, for example, in the shipping industry [67, 113, 132, 159, 174] and the public sector [71, 86].

However, these prototypes focus on their respective domain only and do not communicate their insights back to the blockchain community. Thus, insights into the design and architecture of blockchain-based document management systems (bDMSs) are scattered across domains. Due to this fragmentation of knowledge, only a few papers provide guidance for the technical implementation of blockchain-based document systems [3]. Nevertheless, architectural recommendations that guide the implementation of bDMS are needed to inform and accelerate document digitization, meeting rigorous quality standards. In order to provide an improved information foundation in this context, it is necessary to identify the architectural approaches and best practices for blockchain-based document management systems across various domains. Therefore, this paper raises the research question: *What are the architectural design choices and methodologies for blockchain-based document management systems?*

We address the research question by conducting a systematic literature review (SLR) of blockchain-based document management systems, analyzing a total of 113 papers, focusing on the implementation aspects and architectural building blocks. Our paper contributes to the existing literature by identifying and delineating the different architectural approaches used. We show that two general architecture archetypes, dApp and proxy-based, are common, but best practices of Blockchain-Oriented Software Engineering (BOSE) or general software engineering are not applied. The current research outcomes lack maturity as they seldom go beyond conceptual work or prototypes. Furthermore, the existing technical designs insufficiently consider contextual factors, especially legal regulations.

Therefore, future research should follow a problem-oriented approach and tackle issues that are relevant to practice. In doing so, research can reach higher maturity levels and develop more practical impact. The potential for impact will be further increased by following best practices for designing and engineering bDMS. Synthesizing the recommendations, we outline a future research agenda with the topic areas of software engineering, security and testing, legal, scientific rigor, and application domains. In summary, the paper contributes to the field by laying the foundation for successful implementation of blockchain-based document management systems, enabling researchers and practitioners to build upon our findings.

2 BACKGROUND: DOCUMENT MANAGEMENT SYSTEMS AND BLOCKCHAIN

Early research on enterprise document management already identified the necessity of actively managing documents decades ago [138]. Documents are “recorded information structured for human consumption” [78]. They

[1] https://www.mordorintelligence.com/de/industry-reports/enterprise-content-management-market (accessed: 2024-05-28)
[2] https://www.marketsandmarkets.com/Market-Reports/enterprise-content-management-market-226977096.html (Id.)
[3] https://www.fortunebusinessinsights.com/industry-reports/enterprise-content-management-ecm-market-101660 (Id.)

comprise primarily text, but electronic documents can also include images, audio, or video [138]. Organizations must deal with vast quantities of information and documents and increasing regulatory requirements [136]. As a result, document management has become an integral aspect of contemporary information management in organizations [155].

DMSs provide simplified management of documents that is more effective, has fewer errors, takes less time, is more accurate and consistent along the document lifecycle (i.e., capture, organize, process, and maintain) than paper-based document management [136, 139]. Advantages of DMSs include overcoming the scale ceiling of paper-based document management [10, 90], linking documents with other forms of (multi)media, and interoperability with other systems from an organization. Furthermore, they provide special functionality for dealing with legal documents. Although extended requirements related to authenticity and access control can be implemented in DMSs [3, 136], integrity and transfer of ownership for digital documents remain challenging.

It is difficult to assure that a digital asset is not transacted more than once, a problem which is generally known as the *double-spending problem* [142, 170]. With the development of Bitcoin, Nakamoto [95] showed that the the double-spending problem can be solved by using *a* blockchain and proof-of-work consensus algorithms. This approach paved the way for the representation and transfer of ownership of digital assets.

Thus, blockchain technology with its additional inherent attributes of immutability, non-repudiation, data integrity, and transparency [43] poses potential for DMSs.

From a technical perspective, a blockchain is a data structure implemented as an ordered list of blocks, with each new block cryptographically "chained" to the previous block [166]. Each block can hold transactions that become immutable and persistent, guaranteed through cryptographic functions [166]. This prevents tampering with information [142, 166] which is necessary for DMSs and document integrity. Following peer-to-peer principles, blockchains are decentralized where each participating node that possesses the necessary information and client software can execute transactions on the blockchain [147]. To ensure a consistent state of the blockchain across the nodes, consensus algorithms are employed, solving the double-spending problem [142, 176]. Therefore, the representation and ownership transfer of digital documents is possible.

However, blockchain is not a panacea. Blockchain leads to higher complexity, lacks scalability, and – paradoxically – has problems with storing large quantities of unstructured data, e.g., documents [166]. There are two main approaches to storage in blockchain-based systems: Storage *within* the blockchain is called on-chain vis a vis storage *outside* the blockchain, which is described as off-chain storage [166]. By leveraging off-chain storage, only references are stored on-chain while the actual data is stored and managed off-chain. Therefore, off-chain storage resolves, at least partly, the scalability and storage limitations of blockchain [39]. In this architecture, blockchain is no longer considered as a storage medium but rather a means to secure an immutable audit trail of references [150].

It follows that blockchain technology must be integrated into an overarching DMS to reap its benefits—transforming it into a bDMS. Architecturally, two patterns exist for blockchain-based systems, namely proxy-based architectures and decentralized Application (dApp)-based architectures [121]. Within a proxy-based architecture, a proxy component is introduced between the client/front-end and the blockchain layer [121]. It enables a separation of concerns and allows for additional functionalities [121].

In a dApp architecture, the client communicates directly with the blockchain layer. The main business logic resides on the client and smart contract (SC) side, focusing on decentralization while accepting a negative trade-off in scalability [121]. dApp-based architectures can further be distinguished into (1) self-generated transactions, (2) self-confirmed transactions, and (3) delegated transactions [161]. We do not consider the subdivision of the dApp pattern to be relevant in the context of this study, so we stick to the umbrella term dApp architecture.

The choice of architecture significantly determines the trade-offs between decentralization, scalability, and other system characteristics. For example, SC support is required if a system must run business logic on-chain. SCs might rely on external (off-chain) data. This data can be made available to the SC via oracles, which are

Table 1. Taxonomy of the SLR with highlighted categories relevant for this paper (following Cooper [28])

Characteristics	Categories			
Focus	research outcomes	research methods	theories	applications
Goal	integration	criticism	identification of central issues	
Perspective	neutral representation		espousal of position	
Coverage	exhaustive	exhaustive/selective	representative	central/pivot
Organization	historical	conceptual	methodological	
Audience	specialized scholars	general scholars	practitioners	general public

distinguished into four types: *inbound-pull*, *outbound-pull*, *inbound-push*, *outbound-push* [92]. Each type defines a communication pattern between the on-chain and the off-chain component.

Since many decisions pertaining to architectural design must be made, rigorous system analysis and design are key to successfully implementing any blockchain-based system. Traditional software engineering methods are employed in the development of blockchain-based systems [66]. However, given the specific characteristics of blockchain-based systems, tailored approaches are necessary. To this end, BOSE, initially coined by Porru et al. [111], emerged. As part of this, ABCDE, developed by Marchesi et al. [87], is an agile method for dApp development [18, 87] and *Blockchain-Oriented Software Engineering Approach for Higher Adoption Possibility (BOSE-HAP)* enhances the adoption of blockchain systems [81].

Additionally, specific tests are required for blockchain-based systems, such as SC testing or blockchain transaction testing (BTT) [111]. SC testing comprises functional, performance, and security testing of the respective SCs [88]. BTT refers to "tests against double spending and to ensure status integrity [...]" [111].

The type of blockchain technology impacts the design of the architecture. For example, common technologies used for bDMSs include Ethereum and Hyperledger Fabric. While Ethereum was developed as a public permissionless blockchain, Hyperledger Fabric was developed for enterprise usage as a private permissioned blockchain. Hence, these two systems differ in the used consensus algorithms, transaction costs, and transaction throughput.

Although there are SLRs for blockchain usages for certain domains, e.g., supply chain [22, 41] or industry [80], they do not investigate bDMS but only blockchain in general. They do not focus on system analysis and design or offer best practices for the design and architecture of bDMSs. This underlines the need to investigate the architectural building blocks for blockchain-based document management systems.

3 SYSTEMATIC LITERATURE REVIEW

In order to implement our investigation, we conducted a SLR. We categorized the SLR according to the taxonomy of Cooper [28] in Table 1. The focus lies on research outcomes and applications, as our goal is to identify the state of the art of bDMS by examining existing architectures and methodologies. We take a neutral perspective not to limit the scope of our review—we only espouse positions when suggesting recommendations for the field from the synthesized literature. We selected an exhaustive but selective coverage, including most of the literature, but only presenting the most relevant ones due to space limitations [28]. Since our goal is to elaborate on the used architectures for bDMS, the organization of our review is conceptual. Finally, our target audiences are specialized scholars and practitioners alike, for whom the recommendations are relevant.

The implementation of the SLR followed the guidelines from Kitchenham and Charters [70] and vom Brocke et al. [156, 157]. We performed a three step-process, adapting the steps: (1) definition of keywords and search terms, (2) identification and selection of papers by performing keyword search, and (3) analysis of relevant papers [160]. We further utilize the PRISMA method to present our SLR [102].

Table 2. Overview of used search terms per databases

Database	**Search Term**
ACM Digital Library	*blockchain* within abstract, *"digital document"? OR "electronic document"? OR "document"?* in full text
IEEE Xplore	*("All Metadata":blockchain) AND (("All Metadata":"digital document") OR ("All Metadata":"electronic document")) OR (("Full Text Only":blockchain) AND (("Full Text Only":"digital document") OR ("Full Text Only":"electronic document")))*
Science Direct	*"blockchain" AND ("digital document" OR "electronic document")*
AIS eLibrary	*all fields: blockchain digital documents OR electronic documents*
Springer Link	*"blockchain" AND ("digital document" OR "electronic document")*

3.1 Definition of Search Terms and Selection of Databases

We created a set of search terms to query scientific databases and gathered an initial set of literature to review. The keywords used in the search terms were kept loose and abstract because we aimed for an exhaustive review. Therefore, we chose the following keywords: *blockchain*, *digital document*, and *electronic document*. These keywords were combined with boolean logical operators to form the search queries (Table 2). We queried a total of five databases or repositories that are well known in the information systems (IS) and computer science (CS) communities, namely *ACM Digital Library*, *IEEE Xplore*, *AIS eLibrary*, *Science Direct* and *Springer Link*. The combination of these databases or repositories ensures an exhaustive coverage of published findings. The search was carried out in February 2024. Table 2 shows the search terms for each database. Minor changes in the search terms are caused by differences in the syntax of the databases or repositories. The advanced search features of the respective databases were used where possible. After the initial search, we extended the resulting set of papers with one round of forward- and backward-search to increase the coverage. We follow the PRISMA approach for reporting the filtering and result set of our literature review [102](Figure 1). After gathering the initial papers based on the keyword search, we conducted a two-step process to identify the relevant papers for this research and filter out the rest. First, we screened the papers' abstracts. By screening the abstracts, the general relevance of the paper in the context of bDMS was assessed. If the abstract uncovered that the paper did not fit the scope of this study, the paper was excluded from further consideration. Conversely, if the abstract showed that the paper dealt with blockchains for document digitization, we scrutinized its full text. While checking the papers' full texts, we evaluated whether they proposed an architecture or implementation for bDMS. If a paper merely provided a superficial discussion of the topic without proposing a dedicated architecture or implementation, it was discarded from further consideration. Therefore, the resulting set of papers focused on papers that describe concrete systems and architectures. Finally, only papers that were written in English and peer-reviewed were considered to ensure the quality of our findings. After screening the abstract, 312 papers remained. After scrutinizing the full text, 113 papers remained for detailed coding of the results as shown in Figure 1.

3.2 Coding of Papers

The literature search covered a broad range of manuscripts to be as comprehensive as possible to answer our research question about the architectural building blocks for bDMSs. The coding procedures must be aligned with this approach to identify and describe the entire extent of architectures and implementations in bDMSs. As a result, we followed the recommendations for a scoping review by Paré et al. [106] to map the research field, distill recommendations, and develop a research agenda. Accordingly, we derived a deductive coding schema from the blockchain architecture variants introduced in section 2 (Table 3). The qualitative content analysis of the scoping

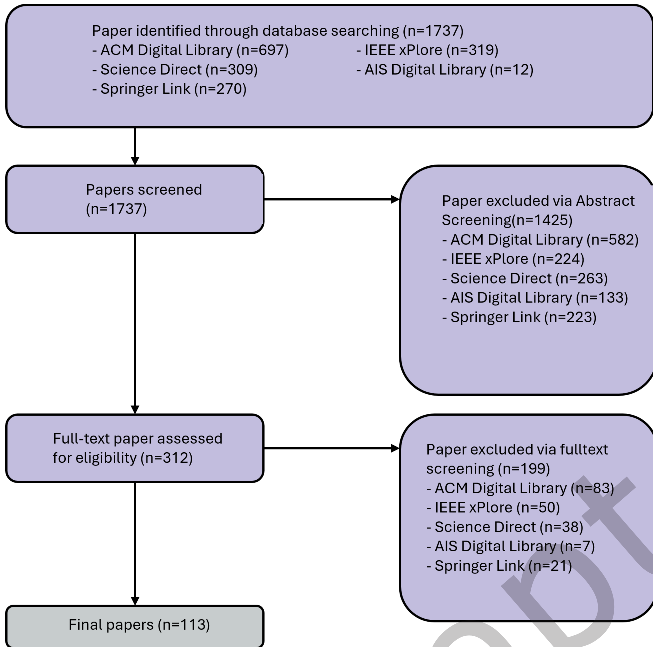

Fig. 1. PRISMA flow diagram adopted from Page et al. [102]

review is based on two coding rounds to structure and filter the papers according to the coding schema [89]. In the first round of descriptive coding, the first author assigned codes to all papers [128]. The codes were verbatim extracted from the papers that explicitly addressed the coding categories. Papers may not have mentioned the respective codes but implemented them implicitly. During our full-text screening, we assessed those implicit codes and grouped them with the explicit ones. In the second round of consensual coding, the authors jointly discussed and agreed on each code to yield the final set of codes [72]. The results and tables are generated from this final set of codes. The detailed rationale for coding each referenced paper is provided in the appendix in Table 14.

4 RESULTS OF THE SYSTEMATIC LITERATURE REVIEW

For each coding category, a dedicated section presents the respective findings and explanations. We observe an increase of relevant publications in the realm of bDMS over time, as shown in Figure 2. The year 2022 peaked in terms of publication counts, with a total of 31 publications. The drop in the year 2024 is based on the time this review was conducted (February, 2024).

4.1 Architecture: Design, Patterns and Software Engineering

For the first coding category, *architecture*, we follow the two main distinctions: proxy-based architecture and dApp-based architectures [161, 166], displayed in Table 4. If we could not identify an architecture, the paper was mapped to *n.a.*. As shown in Table 4, the proxy architecture is the most used architecture (*48%*, n=54). This architecture is necessary if legacy systems or enhanced functionalities are required. For example, Wang et al. [158] and Rukanova et al. [125] enabled the connection of legacy and ERP systems for data imports via a back-end component. Nguyen et al. [96] and Pal and Kumar [103] leverage the proxy architecture approach to include a

Table 3. Coding Scheme for bDMS

Coding Category	**Explanation**	**Justification**
Architecture	Which blockchain architecture patterns are used?	The used architectural patterns highlight how bDMSs can be designed from which best practices can be derived.
Storage	Is document data stored on- or off-chain?	Storing document data on- or off-chain has implications for the architecture of the bDMS, the data flow as well as legal compliance.
Technology	Which blockchain technology is used for the bDMS?	The blockchain technology determines how the blockchain must be integrated into the bDMS with implications for application programming interfaces.
Domain	In what domain are bDMSs used?	Various domains adopted blockchain for bDMS with insights about the generalizability and feasibility of architectural patterns.
Maturity	In what development state is the proposed system?	The maturity provides insights into whether the architectures of bDMS work in live production systems and provide sufficient scalability and legal feasibility.

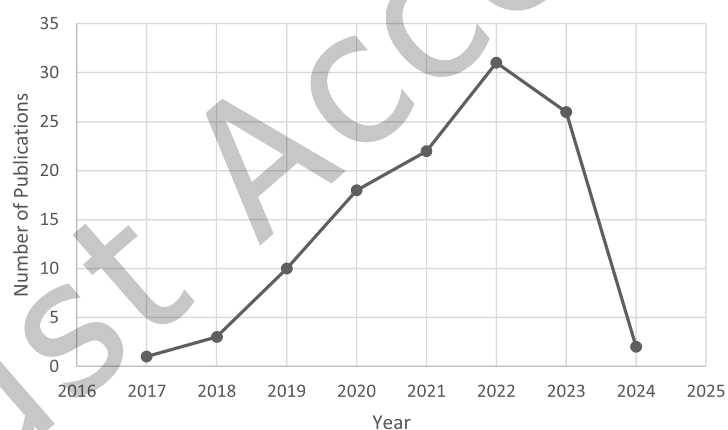

Fig. 2. Number of Publications over Time

QR code functionality to ensure document authenticity in case of a printout. The dApp architecture was used *38%* (n=43) of the time, while *14%* (n=16) provided no insight regarding general architecture design.

Best practices, design patterns, and testing strategies are important for bDMS because they deal with potentially important, valuable, and personal documents [34]. To this end, Porru et al. [111] proposed BOSE, which includes such practices and patterns that addresses the highlighted need for "novel approaches to development of blockchain applications" [14]. In this review, the practices and patterns from BOSE that we identified include

Table 4. Overview of used architectures, dApp vs. proxy

Architecture	Primary Studies
Proxy (n = 54)	[165], [148], [57], [24], [5], [25], [48], [99], [158], [91], [125], [134], [175], [104], [154], [127], [47], [74], [137], [141], [123], [50], [168], [12], [19], [54], [122], [94], [110], [63], [21], [177],[36], [144], [116], [117], [73], [130], [32], [49], [60], [79], [27], [65], [69], [93], [76], [51], [173], [29], [140], [64], [53], [85]
dApp (n = 43)	[145], [96], [109], [152], [143], [40], [100], [1], [55], [52], [6], [59], [133], [120], [101], [164], [26], [163], [20], [126], [151], [98], [97], [131], [77], [107], [33], [11], [62], [75], [61], [105], [2], [162], [129], [114], [38], [35], [17], [56], [171], [30], [31],
n.a. (n = 16)	[112], [7], [135], [118], [4], [83], [8], [9], [68], [153], [169], [119], [172], [37], [82], [103]

the oracle (Table 5) and testing patterns (Table 6), the reporting of SCs (Table 7), and the application of an established software engineering methodology (Table 8). As bDMS systems require input from the outside world

Table 5. Overview used oracle patterns

Oracle pattern	Primary Study
Implicit use of oracle pattern (n = 93)	[125], [24], [48], [99], [158], [91], [40], [100], [177], [144], [36],[131], [97], [77], [21], [175], [52], [154], [6], [127],[172], [59], [133], [120], [101], [47], [74], [137], [29], [140], [123], [50],[164], [26], [64], [73], [130], [112], [107], [32], [7], [33], [135], [49], [11], [53], [118], [75], [4], [60], [61], [79], [83], [105], [27], [8], [65], [62], [63], [76], [31], [37], [98], [82], [2], [162], [129], [114],[163],[168], [103],[12], [19], [20], [85], [54],[30], [126], [122], [94], [110], [151], [38], [9], [69], [17], [56], [171], [93], [68], [153], [169], [119]
Implicit use of inbound-push (n = 16)	[51], [165], [148],[145], [134],[57], [25], [5], [96],[109], [152], [55], [173], [116], [117], [104]
Explicit mention of inbound-push (n = 4)	[143], [1], [141], [35]

(e.g., document information or metadata), we expected explicit mentions of the oracle patterns. However, the findings show that *82%* (n=93) of all analyzed papers did not report on any usage of the oracle pattern (Table 5). If the analyzed paper did not explicitly mention any used pattern, we derived their existence based on the reported infrastructure and information flow (if provided). *14%* (n=16) of the papers used oracle patterns based on their presentation of information flow. Only *4%* (n=4) of the papers explicitly stated the respective oracle pattern.

The assurance of functionality, correctness, and thus the security of bDMS is important for handling valuable documents. Beyond the traditional software engineering testing patterns, blockchain-oriented systems require additional testing focused on SCs. Following Marijan and Lal [88], we distinguish functional, performance, and

Table 6. Overview of used SC testing pattern

SC testing pattern	Primary Study
n.a. (n = 88)	[125], [165], [148], [145], [134], [57], [5], [96], [48], [152],[55], [158], [91], [40], [100], [1], [144], [116], [97], [117], [175], [104], [154], [127], [172], [59], [133], [120], [101], [47], [74], [137], [29], [140], [123], [50], [164], [26], [64],[73], [130],[112], [107], [32], [7], [135], [49], [11], [53], [118], [75], [4], [60], [61], [79], [27], [8], [65], [63], [76], [37], [82], [2], [162], [129], [163], [168], [103], [19], [20], [85], [54], [30], [126], [94], [110], [151], [9], [35], [69], [17], [171], [68], [153], [119]
Implicit use of performance testing (n = 15)	[51], [177], [36] [109], [99], [173],[6], [33], [83], [114], [12], [122], [38], [169],[56],
Explicit mention of performance testing (n = 5)	[24](caliper), [21](JMeter), [131], [52], [141] , [31],
Explicit mention of SC security testing (n = 4)	[25], [77], [105] (Scyther), [98] (ChainSecurity)
Explicit mention of SC testing (n = 3)	[143] (Proverif), [62] (Mocha), [93] (Mocha)

Table 7. Overview of used SC description

Reporting on Smart Contracts	Primary Study
Functional description (n = 64)	[51], [165], [148], [134], [5], [24],[152], [99], [55], [143], [173], [158], [91], [100], [1], [177], [144], [36], [131], [116], [97], [117], [175], [104], [154], [6], [59], [133], [120], [101], [47], [74], [137], [29], [123], [50], [26], [112], [33], [135], [11], [53], [4], [61], [79], [83], [105], [98], [82], [114], [163], [168], [20], [54], [94], [110],[151], [35], [17], [153]
n.a (n = 35)	[125], [145], [57], [48], [40], [172], [140], [164], [64], [73], [130], [32], [7], [49], [118], [75], [27], [8], [65], [63], [76], [37], [103], [12], [85], [126], [122], [38],[9], [69], [56], [93], [68], [169], [119]
Code (n = 9)	[25], [77],[141], [107], [60], [2], [129], [19], [171]
Pseudo code / diagram (n = 9)	[96], [109], [21], [52], [127], [62],[162], [30]. [31],

security testing patterns for SCs (Table 6). *78%* (n=88) of the papers neither explicitly nor implicitly report on the use of any testing patterns. For *13%* (n=15) papers, we were able to deduce the implicit use of performance testing. When it comes to explicitly stated testing patterns, only *4%* (n=5) mentioned the usage of performance testing, another *4%* (n=4) of the papers stated to use existing tooling for security testing, and only *3%* (n=3) of the papers reported explicit smart contract testing.

In light of the low number of tools used to support SC testing and quality, we further assess the general presentation of SC related information in the literature. Table 7 shows that *57%* (n=64) of the papers report on a textual level about the used or developed SCs while *31%* (n=35) do not present any details regarding SCs. Only *8%* (n=9) and *8%* (n=9) of the papers report SC details on a code or pseudo-code level.

Table 8. Overview of used SE methodology

Software Engineering Methodology	**Primary Studies**
n.a. (n = 112)	[51], [125], [165],[148], [145], [134], [57], [25], [5], [96], [24], [109], [48], [152], [99], [55], [143],[173], [158], [91], [40], [100], [1], [177], [144], [36], [131], [116], [97], [117], [77], [21], [175], [104], [52], [154], [6], [127], [172], [59], [133], [120], [101], [47], [74], [137], [29], [140], [141], [123],[50], [164], [26],[64], [73], [130], [112], [107], [32], [7], [33], [135], [49], [11], [53], [118], [75], [4], [60], [61], [79], [83], [105], [27], [65],[62], [63], [76], [31], [37], [98], [82], [2], [162], [129], [114], [163], [168], [103], [12], [19], [20], [85], [54], [30], [126], [122], [94], [110], [151], [38], [9], [35], [69], [17], [56], [171], [93], [68], [153], [169], [119]
Rapid application development (n = 1)	[8]

The application of established software engineering methodologies was not reported, except for one paper that used rapid application development (Table 8). *99%* (n=112) did not mention *any* software engineering-related method in their approach. Neither agile methods such as scrum nor "traditional" approaches such as waterfall are mentioned. In particular, BOSE specific approaches such as ABCDE are not reported for the development of bDMS.

4.2 Storage

Table 9 shows that *68%* (n=77) of the papers leverage off-chain storage. Considering off-chain storage, *36%* (n=41) of the approaches use the Interplanetary File System (IPFS) protocol, making use of a distributed hash table (DHT), so no centralized storage is required. Next to IPFS, traditional, relational databases are used (*15%*, n=17). For example, Xue et al. [168] rely on a MySQL database.

There is consensus that blockchain is no longer considered a storage medium because storing data directly on the chain has significant drawbacks related to privacy (e.g., GDPR) and scalability [150]. Nevertheless, *22%* (n=25) of the papers still rely on on-chain storage. *27%* (n=30) of the papers used other off-chain approaches or did not describe how they stored data.

4.3 Technology

The most used underlying blockchains are Ethereum (*50%*, n=56) and Hyperledger Fabric (*27%*, n=30). This finding is expected because these blockchains are popular [108]. Most of the approaches relying on Ethereum use public Ethereum except for Toyoda et al. [148], Pongnumkul et al. [109], Norvill et al. [99], and Heredia and Barros-Gavilanes [55] who rely on a private Ethereum setup. The studies listed as *n.a.* (*12%*, n=14) propose general frameworks or ideas but do not provide an actual implementation (Table 10). *12%* (n=14) of the papers used other blockchain technologies.

4.4 Domain

Table 11 shows that *34%* (n=38) of the papers developed a bDMS for academic certificates, while *25%* (n=28) of the studies sought general applicability. For example, Jovović et al. [64] present a bDMS that allows for

Table 9. Overview of used storage systems

Storage system	**Primary Studies**
Off-chain, IPFS (*n* = 41)	[148], [145], [57], [24], [25], [152], [175], [104], [6], [127], [59], [133],[164], [26], [19], [20],[30], [126], [122], [31], [98], [21],[177], [135], [11], [62], [53], [61], [83], [27], [65], [162], [129],[114], [35], [17], [153], [169], [119], [173], [82]
On-chain (*n* = 25)	[109], [158], [40], [1], [55], [52], [120], [101],[151], [94], [97], [131], [117], [32], [75], [105], [2], [38], [9], [171], [172], [103], [85], [163],[56],
Off-chain, relational database (*n* = 17)	[48], [99], [134], [141], [123],[168], [54], [110], [63], [36], [144], [116], [64], [93], [51],[29], [140]
n.a. (*n* = 11)	[100], [47], [50], [130], [112], [107], [7], [49], [118], [4], [37]
Off-chain, cloud storage (*n* = 6)	[165], [5], [91], [125],[73], [68]
Off-chain, NoSQL database (*n* = 5)	[74],[12], [33], [79], [8]
Off-chain (*n* = 4)	[77], [60], [69], [76]
Off-chain, digital wallet (*n* = 3)	[96], [143], [154]
Off-chain, GAIA (*n* = 1)	[137]

Table 10. Overview of used blockchain systems in the studies

Blockchain	**Primary Studies**
Ethereum (*n* = 56)	[165], [148], [96], [25], [109], [152], [99], [143], [100], [1], [55], [104], [52], [6], [59], [133], [120], [47], [141], [50], [163], [168], [19], [20], [30],[98], [97], [36], [131], [77], [64], [107], [32], [7], [33] [135], [11], [53], [75], [4], [60], [61], [105], [2], [162], [114], [35], [17], [171], [93], [68], [153], [119], [51], [173], [140], [83]
Hyperledger Fabric (*n* = 30)	[145], [24], [5], [158], [40], [125], [134], [175], [74], [123], [164], [26], [54], [122], [94], [31], [63], [21], [177], [144], [116], [49], [27], [65], [38], [56], [76], [37]
n.a. (*n* = 14)	[127], [126], [110], [151], [117], [73], [112], [118], [8], [9], [69], [82], [103], [85]
Blockchain agnostic (*n* = 5)	[57], [169], [154], [172], [79]
Polygon Matic (*n* = 2)	[62], [129]
Bitcoin (*n* = 1)	[48]
Hyperledger Iroha (*n* = 1)	[91]
Blockstack (*n* = 1)	[137]
Mystiko (*n* = 1)	[12]
IOTA (*n* = 1)	[130]
PrivateSKY (*n* = 1)	[29]
MultiChain (*n* = 1)	[101]

Table 11. Overview of domains

Domain	**Primary Studies**
Academic certificates (*n* = 38)	[96], [143], [40], [1], [55], [104], [120], [47], [74], [123], [20], [122], [151], [36], [117], [77],[64], [73], [7], [33], [135], [49], [4], [83], [27], [65], [114], [38], [9], [56], [171], [93],[68], [119], [140], [37], [82], [154]
General applicability (*n* = 28)	[148], [57], [5], [25], [152],[52], [6], [127],[59], [137], [50], [26], [168], [19], [98], [116], [107], [32], [118], [75], [61], [35], [153], [51], [172],[29], [103], [85]
Miscellaneous (*n* = 12)	[99], [100], [177], [12], [101], [164], [163], [24], [130], [162], [17], [79],
Land administration (land mortgage/registry/property) (*n* = 8)	[109], [48], [134], [133], [144], [112], [53], [169], [141]
Healthcare (*n* = 9)	[165],[145], [54],[21], [97], [131], [62], [60], [173]
Personal documents (*n* = 7)	[91],[126], [94], [105], [8],[2], [129]
Construction (*n* = 6)	[175], [30], [31], [11], [69], [76]
Logistics/shipment (*n* = 4)	[158], [125], [110], [63]

requesting, creating, and receiving digital diplomas. More frequent domains include land administration (land mortgage/registry/property) (*7%*, n=8), healthcare (*8%*, n=9), personal documents (*6%*, n=7), construction (*5%*, n=6), and logistics/shipment (*4%*, n=4). For example, Vashistha and Barbhuiya [152] present a generalized system for bDMS, which aims to be suitable for all kinds of documents and is based on IPFS and Ethereum. For the domain of land administration, Hasan et al. [53] discussed a system for land deed verification and reservation in Bangladesh. As an example from healthcare, He et al. [54] developed BlockMed, a blockchain-based online prescription system to overcome the current limitations of paper-based prescriptions. In the domain of personal documents, Naimur Rahman et al. [94] proposed a blockchain-based system for international driving permits and traffic crime reporting systems. Zhao et al. [175] described a bDMS for construction documents in infrastructure projects based on Hyperledger and IPFS. Considering the domain of Logistics/Shipment, Ponza et al. [110] described a bDMS focused on the management of Bills of Exchange. *11%* (n=12) of the papers target other domains.

4.5 Maturity

The last coding category is *maturity*, illustrated in Table 12. Only 2% (n=2) of the systems are in a production stage [63, 125], meaning that the system is deployed and used in live systems and processes. 3% (n=3) of the systems are in the pilot stage [48, 100], that is, a built prototype is used and evaluated in a live environment, showing the potential for long-term usage and integration. 81% (n=91) of the papers reported a prototype, that is, the described technical implementation is used to prove technical feasibility in the form of a prototype implementation. Finally, 15% (n=17) of the studies proposed a bDMS with no implementation undertaken.

5 DISCUSSION

The number of papers building bDMSs show that blockchain technology offers useful features to enhance DMSs. Blockchain's immutability and consensus mechanisms overcome the issues of forgery, tampering, and the transfer of ownership from which digital, non-blockchain DMS suffer. Nevertheless, due to blockchain's scalability issue,

Table 12. Overview of development states

Development State	Primary Studies
Prototype (n = 91)	[165], [148],[145], [24], [5], [96], [25], [109], [152], [99], [143], [158], [91], [40], [1], [55], [134], [175], [104], [52], [154], [6], [127],[59], [101], [47], [74], [137], [141], [123], [50],[164], [26], [163], [168], [12], [19], [20],[54], [30], [94], [31], [21], [177], [97], [36], [131], [144], [116], [77], [64], [130], [107], [32], [7], [33], [135], [11], [62], [53], [75], [4], [60], [61], [79], [83], [105], [27], [65],[2],[162], [129], [114], [38], [35], [69], [17], [56], [171], [93], [68], [153], [169], [119], [76], [51], [173], [29], [140], [122], [98]
Proposal (n = 17)	[57], [133], [120], [126], [110], [151], [117], [73], [112], [49], [118], [8], [9], [172], [37], [103], [85]
Pilot (n = 3)	[48], [100], [82]
Product (n = 2)	[125], [63]

the blockchain must be integrated into an overarching DMS. This overarching system allows for many choices pertaining to architecture, storage, technology, and testing.

5.1 Architecture and Software Engineering

We found that 86% of the analyzed papers (implicitly) reported on the general usage of either the proxy or dApp architecture. Zooming in on the design of the respective bDMS and related SCs, however, we found that most papers do not explicitly describe their implementation or methodology. Only *16%* (n=18) of the papers provide details into the designed or developed SC by providing code or pseudo code listings.

Despite blockchain developers acknowledging the existence of the BOSE methodology or ABCDE, these approaches are not being adopted [18, 87]. In the context of bDMS development, *99%* of the surveyed papers did not mention BOSE or *any* other software engineering methodology. Rigorous requirements engineering is absent from the surveyed papers. Instead, most papers only provide a superficial justification for blockchain being tamper-proof and preventing forgery. 78% of surveyed papers did not mention any actions regarding testing, quality assurance, or SC testing, although recommendations, standards, and established development approaches exist [14, 111]. Existing methods and tooling support to tackle known vulnerabilities are not applied [23, 88]. These findings support Khalid and Brown [66], who showed that only 14% of their survey respondents recognized the need for secure coding practices even though they were dealing with valuable assets. These findings are concerning, as the surveyed studies dealt with sensitive, important, or valuable documents (e.g., academic certification, land registries, or health-related data). Similar security concerns were observed in blockchain for IoT [84]. We concur with Treiblmaier [149], who calls for more rigor in the justification, design, implementation, and validation of blockchain use cases.

The surveyed papers focused on the technical possibility of implementing a bDMS and neglected proper communication in terms of software engineering-related elements. Nearly none of the works provided a link to GitHub or other code repositories for the developed system, resulting in minor intersubjective reproducibility. The open science movement encourages transparency. Public code would make it easy to verify the justification, design, and validation of prototypical implementations in a scientific manner.

The lack of rigorous development and communication of results is troubling because demonstrating adherence to best practices, design patterns, and testing is important [34]. We call for more rigorous and reproducible blockchain studies in the future and suggest adding *architecture* and *patterns* as additional elements to the checklist developed by Treiblmaier [149].

5.2 Choosing an Architecture

Practitioners looking to implement a bDMS must choose between a proxy-based and dApp-based architecture. While both architectures are viable, the optimal choice depends on the specific use case.

dApp-based architectures do not require a trusted proxy, making them suitable for low-trust domains. However, the business logic typically resides in SCs on-chain, which can lead to limitations in terms of security and scalability. In the context of this review, we showed that dApp based architectures are commonly used for certificate and credential management such as land registries, personal credentials, or identity management [96, 109, 120, 133, 143]. Other suitable use cases for dApp-based architectures are digital currencies and finance-related documents [15] or audit trails for quality management [58, 162].

Proxy-based architectures implement a trusted proxy as middleware between users/applications and the blockchain layer. Through a proxy, laws, procedures, and safeguards can be dynamically enforced at scale. Scaling is achieved through transactions being processed in batches or buffers. Suitable use cases for proxy-based architectures identified in this review include patient health documents [165], enterprise data with a high number of large documents and files, or sensitive documents [24, 57, 148]. Proxy-based architectures have successfully been integrated with legacy systems in use cases for complex enterprise and industry systems.

5.3 Legal Considerations

Although 34% of the analyzed papers focused on academic certificates subject to the General Data Protection Regulation (GDPR), none considered potential legal implications. The critical impact of the GDPR to blockchain-based systems, especially due to the immutability property, is well-known [39, 124, 178]. Given the immutability property, rules such as the right of erasure cannot be fulfilled, especially when data is stored on-chain. This is crucial, considering that 22% of the analyzed approaches still leverage on-chain storage, rendering them potentially non-GDPR compliant. A possible explanation is that many of the surveyed papers do not originate from within the European Union or countries with similar data protection laws. The EU itself investigates and pushes an active discussion of GDPR compliant blockchain systems [44]. Currently, the common best practice is to leverage off-chain storage without storing personal information on-chain, as shown for example in [46]. However, off-chain storage solutions such as IPFS are also subject to GDPR requirements. Approaches that use cryptography to encrypt data stored on-chain are not deemed GDPR compliant [45]. As analyzed and described by Fridgen et al. [45] in their report for the German Federal Ministry of Transport and Digital Infrastructure, encrypted on-chain data is stored *ad infinitum.* This means that the encryption algorithm could eventually be broken, making the data from that point in time publicly accessible, which may violate the GDPR [45, 115]. In the future, legal compliance, especially GDPR, will be a major requirement to fulfill before bDMS are ready for real-world adoption and use.

5.4 Domains and Maturity

The realm of digital trade documents is an active field of research in logistics [67, 113, 132, 159, 174]. Hence, we expected to find bDMS papers addressing the digitization of trade and legal documents. However, based on our review, only 4% of the papers dealt with document digitization in the logistics sector. This calls for another, more focused review in the future. Such a review might incorporate grey literature because this study does not include potentially existing bDMS approaches from the industry.

Currently, most research projects remain in a pilot or proposal stage regardless of architecture or technology, yielding little technology-readiness in bDMS for practice. As shown in section 4.4, the only two projects in product-stage relate to bDMS for trade documents [63, 125], and the three projects in pilot-stage address property registration, certificates, and legal contracts [48, 82, 100]. Many prototypes focus on academic certification or the general applicability of bDMS for managing digital documents. Contrary to the domain, the type of technology and the architecture seem unrelated to the maturity level.

The lack of maturity has adverse effects, such as wasted resources, lack of practical relevance, and missed market opportunities, leading to stagnating innovation in the field of bDMS. The reason may be that researchers with short-term funded projects are not incentivized to develop their prototype into a viable product. Alternatively, the business case for the concepts and prototypes may be insufficient in practice.

To advance the maturity of bDMS, future research should focus on strong business cases and refine and scale prototypes toward pilots and products. Researchers should engage with practice and espouse a problem-driven, not solution-driven, mindset that considers the product lifecycle and practical relevance.

Summarizing, bDMS offer a compelling alternative to traditional DMS. However, we identified multiple concerns regarding the rigorous design, implementation, and validation of the prototyped systems. The outlined concerns drive our research agenda for the future of bDMS (Table 13) that is presented in the following section.

6 RESEARCH AGENDA

Future research should investigate the reasons behind the reluctance to adopt best practices in bDMS, exploring technical and organizational barriers, and extending prior research such as Batubara et al. [13] and Tanha et al. [146].

Upcoming case studies on bDMS should provide a rigorous justification, design, and validation of their software development efforts based on established blockchain-oriented software engineering approaches. Future research can uncover which software development approaches, e.g., BOSE, are viable for bDMS. Corollary, it can investigate the implications of absent software development approaches. More rigor will contribute to the academic impact of the bDMS field and its translation to industry practice. For SC designs, future research can explore smart contract designs within specific domains [42] or document types and compare aggregated findings between Ethereum and Fabric-based architectures. Security analyses on public Ethereum contracts are needed to enhance understanding and identify potential vulnerabilities in common architectures.

Future research should investigate which quality and security assurance procedures are viable for bDMS, emphasizing correctness for legal compliance, including audits and traceability. Investigating testing methodologies and validation strategies for bDMS will contribute to the robustness and reliability of bDMS.

Future research should examine the integration of legal aspects into bDMS, particularly concerning features such as legal document management. Even though bDMS hold promises for legal documents, the focus of the surveyed papers is on technical details. However, Beck et al. [14] showed that legal and technical concerns are intricately linked. As a result, research should incorporate and discuss regulatory requirements related to blockchain, decentralized documents, privacy, and ownership during the implementation phase.

Finally, applied research happens in the domain-specific areas. However, the surveyed papers seldom contribute to the overarching discourse on bDMS. Future research should seek generalizable findings for the architecture and design of bDMS beyond a specific domain. We highlight the need for scholarly works to not only focus on their application in specific domains but also share their findings with the broader blockchain community. To allow for broader relevance, novel research should justify the domain and application area under study beyond only highlighting technical and engineering concerns. Following a problem-oriented mindset and engaging with practice should lead to more viable and practically useful outcomes.

Table 13. Research Agenda for bDMS

Topic Area	**Example Questions**
Software Engineering	(1) Why are neither software engineering nor BOSE methodologies used for bDMS development? (2) Are existing software development methodologies suitable for building a bDMS? (3) What are the implications of not using established software development methodologies on bDMS?
Security & Testing	(1) What are the risk factors for bDMS? (2) What security procedures and best practices must be considered to avoid vulnerabilities in bDMS? (3) How can bDMS be effectively tested and validated?
Legal	(1) Which legal requirements are relevant to bDMS beyond the GDPR? (2) What architectures are needed to accommodate legal requirements? (3) What legal concerns are relevant for the blockchain on-chain components, which for the off-chain components?) (e.g., decentralized documents, privacy, ownership)
Scientific Rigor	(1) What academic recommendations are needed for blockchain-based architectures to ensure robust and valid justification, design, and implementation? (2) What are the implications of the current lack of rigor in bDMS? (3) How can more rigor in research be translated into higher practical impact?
Domains	(1) Which insights gained in-domain are generalizable to the broader blockchain discourse? (2) How can knowledge contributions from applied bDMS research be solicited for the blockchain community at large? (3) What changes are needed to increase the maturity of bDMS prototypes towards production-readiness?

7 CONCLUSION

This paper shows that blockchain-based document management systems are researched throughout different domains, leveraging different architectural approaches. We showed that Ethereum and Hyperledger Fabric are commonly used with off-chain storage. The high-level architecture is either designed as a dApp or with a proxy component, where the former is usually used for personal documents, and the latter is used for business and industry applications. Currently, most systems remain in the prototype stage. Since our research question focused on blockchain, other DLT technologies may be investigated in the future, for example, self-sovereign identity (SSI).

The SLR uncovered a lack of scientific rigor and reporting of the architectural designs. We provide recommendations for the field and advocate for the use of rigorous methods in the development of blockchain-based document management systems. We emphasize that thorough reporting, justification, and validation of architecture and design, aligning with the principles of design science, will contribute significantly to the impact of the field and its future practical relevance.

REFERENCES

[1] Antonio Welligton S. Abreu, Emanuel F. Coutinho, and Carla I. M. Bezerra. 2020. A Blockchain-based Architecture for Query and Registration of Student Degree Certificates. In *Proceedings of the 14th Brazilian Symposium on Software Components, Architectures, and Reuse*, Everton Cavalcante, Francisco Dantas, Thais Batista, and Gustavo Pinto (Eds.). ACM, New York, NY, USA, 151–160. https://doi.org/10.1145/3425269.3425285

[2] Aarti Amod Agarkar, Mandar Karyakarte, Gajanan Chavhan, Milind Patil, Rajendra Talware, and Lalit Kulkarni. 2024. Blockchain aware decentralized identity management and access control system. *Measurement: Sensors* 31 (2024), 101032. https://doi.org/10.1016/j.measen.2024.101032

[3] Jaffar Ahmad Alalwan and Heinz Roland Weistroffer. 2012. Enterprise content management research: a comprehensive review. *Journal of Enterprise Information Management* 25, 5 (Sept. 2012), 441–461. https://doi.org/10.1108/17410391211265133

[4] Monther Aldwairi, Mohamad Badra, and Rouba Borghol. 2023. DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 652–657. https://doi.org/10.1109/BCCA58897.2023.10338908

[5] Afnan Alniamy and Bradley D. Taylor. 03122020. Attribute-based Access Control of Data Sharing Based on Hyperledger Blockchain. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*. ACM, New York, NY, USA, 135–139. https://doi.org/10.1145/3390566.3391688

[6] Yasmeen shaher Alslman and Anas Abu Taleb. 2021. Exchanging Digital Documents Using Blockchain Technology. In *2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*. IEEE, 1–6. https://doi.org/10.1109/ICECCE52056.2021.9514253

[7] Shaista Alvi and Mubeena Iqbal. 2023. Academic Credential Authentication on Blockchain: DeLone and McLean model. In *2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 320–325. https://doi.org/10.1109/ICCIKE58312.2023.10131763

[8] Darius Antoni, Muhammad Izman Herdiansyah, Muhamad Akbar, Widya Cholil, and Hadi Syaputra. 2022. Use of Blockchain for Designing Digital Documents in Public Services. In *2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE, 55–60. https://doi.org/10.1109/ICIMCIS56303.2022.10017661

[9] Vijay Anant Athavale, Shakti Arora, and Anagha Athavale. 2022. Adoption of Blockchain Technology for Storage and Verification of Educational Documents. In *Data, Engineering and Applications*, Sanjeev Sharma, Sheng-Lung Peng, Jitendra Agrawal, Rajesh K. Shukla, and Dac-Nhuong Le (Eds.). Lecture Notes in Electrical Engineering, Vol. 907. Springer Nature Singapore, Singapore, 83–98. https://doi.org/10.1007/978-981-19-4687-5_7

[10] V. Balasubramanian and Alf Bashian. 1998. Document management and Web technologies: Alice marries the Mad Hatter. *Commun. ACM* 41, 7 (jul 1998), 107–115. https://doi.org/10.1145/278476.278498

[11] Shrinivas Baldawa, Lakshmisudha Kondaka, R. Shobhana Iyer, and Divyalaxmi Thiruganan. 2023. Blockchain-based Construction Management System. In *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 597–603. https://doi.org/10.1109/ICOEI56765.2023.10125997

[12] Eranga Bandara, Xueping Liang, Sachin Shetty, Wee Keong Ng, Peter Foytik, Nalin Ranasinghe, Kasun de Zoysa, Bård Langöy, and David Larsson. 2020. Lekana - Blockchain Based Archive Storage for Large-Scale Cloud Systems. In *Blockchain – ICBC 2020*, Zhixiong Chen, Laizhong Cui, Balaji Palanisamy, and Liang-Jie Zhang (Eds.). Lecture Notes in Computer Science, Vol. 12404. Springer International Publishing, Cham, 169–184. https://doi.org/10.1007/978-3-030-59638-5_12

[13] F. Rizal Batubara, Jolien Ubacht, and Marijn Janssen. 2018. Challenges of blockchain technology adoption for e-government. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, Marijn Janssen, Soon Ae Chun, Vishanth Weerakkody, Anneke Zuiderwijk, and Charles C. Hinnant (Eds.). ACM, New York, NY, USA, 1–9. https://doi.org/10.1145/3209281.3209317

[14] Roman Beck, Michel Avital, Matti Rossi, and Jason Bennett Thatcher. 2017. Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering* 59, 6 (2017), 381–384. https://doi.org/10.1007/s12599-017-0505-1

[15] Max Beinke, Jan Heinrich Beinke, Eduard Anton, and Frank Teuteberg. 2024. Breaking the chains of traditional finance: A taxonomy of decentralized finance business models. *Electronic Markets* 34, 1 (April 2024). https://doi.org/10.1007/s12525-024-00704-4

[16] Daimler Benz, Muzaffar Hamzah, Mohd Fahmi Ghazali, and Mohammad Fadhli Asli. 2022. Bringing Blockchain Technology in Innovating Industries: A Systematic Review. In *Proceedings of International Conference on Emerging Technologies and Intelligent Systems*, Mostafa Al-Emran, Mohammed A. Al-Sharafi, Mohammed N. Al-Kabi, and Khaled Shaalan (Eds.). Lecture Notes in Networks and Systems, Vol. 322. Springer International Publishing, Cham, 391–416. https://doi.org/10.1007/978-3-030-85990-9_33

[17] Shreerang Bhat, Pashva Mehta, and Malhar Marathe. 2023. Blockchain-Based System for Storing Warranty Receipts. In *Inventive Communication and Computational Technologies*, G. Ranganathan, Xavier Fernando, and Álvaro Rocha (Eds.). Lecture Notes in Networks and Systems, Vol. 383. Springer Nature Singapore, Singapore, 343–357. https://doi.org/10.1007/978-981-19-4960-9_27

[18] Amiangshu Bosu, Anindya Iqbal, Rifat Shahriyar, and Partha Chakraborty. 2019. Understanding the motivations, challenges and needs of Blockchain software developers: a survey. *Empirical Software Engineering* 24, 4 (2019), 2636–2673. https://doi.org/10.1007/s10664-019-09708-7

[19] Clemens Brunner, Fabian Knirsch, and Dominik Engel. 2020. SPROOF: A Decentralized Platform for Attribute-Based Authentication. In *Information Systems Security and Privacy*, Paolo Mori, Steven Furnell, and Olivier Camp (Eds.). Communications in Computer and Information Science, Vol. 1221. Springer International Publishing, Cham, 1–23. https://doi.org/10.1007/978-3-030-49443-8_1

[20] Sugandha Budhiraja and Rinkle Rani. 2020. TUDocChain-Securing Academic Certificate Digitally on Blockchain. In *Inventive Computation Technologies*, S. Smys, Robert Bestak, and Álvaro Rocha (Eds.). Lecture Notes in Networks and Systems, Vol. 98. Springer International Publishing, Cham, 150–160. https://doi.org/10.1007/978-3-030-33846-6_17

[21] Siriboon Chaisawat, Kajornsak Piyoungkorn, Soontorn Sirapaisan, and Chalee Vorakulpipat. 2022. Towards Data Minimization and Access Control for Immunization Data Sharing. In *Proceedings of the 14th International Conference on Management of Digital EcoSystems*, Ernesto Damiani, Claudio Silvestri, Mirjana Ivanovic, Richard Chbeir, and Yannis Manolopoulos (Eds.). ACM, New York, NY, USA, 16–23. https://doi.org/10.1145/3508397.3564837

[22] Shuchih E. Chang and Yichian Chen. 2020. When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications. *IEEE Access* 8 (2020), 62478–62494. https://doi.org/10.1109/ACCESS.2020.2983601

[23] Hongsong Chen, Xietian Luo, Lei Shi, Yongrui Cao, and Yongpeng Zhang. 2023. Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective. *Blockchain: Research and Applications* 4, 3 (2023), 100135. https://doi.org/10.1016/j.bcra.2023.100135

[24] Li Chen, Kaizhi Chen, Shangping Zhong, and Dongyang Ye. 2019. Privacy Protection Method of Document Management Based on Homomorphic Encryption on the Fabric Platform. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. ACM, New York, NY, USA, 31–37. https://doi.org/10.1145/3376044.3376063

[25] Taowei Chen, Yimin Yu, ZhengTai Duan, Jian Gao, and Kun Lan. 2020. BlockChain/ABE-based Fusion Solution for E-government Data Sharing and Privacy protection. In *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*. ACM, New York, NY, USA, 258–264. https://doi.org/10.1145/3443467.3443764

[26] Sireesha Chiliveri, Jyostna Grandhi, Mahesh Uttam Patil, Lakshmi Eswari P.R., and Magesh Ethirajan. 2019. ProveDoc: A Blockchain Based Proof of Existence with Proof of Storage. In *2019 International Conference on Information Technology (ICIT)*. IEEE, 239–244. https://doi.org/10.1109/ICIT48102.2019.00049

[27] Vaibhavi Chincholkar, Shria Srivastava, Aamey Pawanarkar, and Sheetal Chaudhari. 2023. Skills 360: Machine Learning-Driven Job Recommendation and Immutable Document Verification Through Blockchain Technology. In *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*. IEEE, 1–6. https://doi.org/10.1109/ASIANCON58793.2023.10269905

[28] Harris M. Cooper. 1988. Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society* 1, 1 (1988), 104–126. https://doi.org/10.1007/BF03177550

[29] Catalin Damian, Alexandru Sofronie, and Lenuta Alboaie. 2021. SmartDPO - Template Based, Integrated Flow Document Management System. In *2021 International Conference on Electromechanical and Energy Systems (SIELMEN)*. IEEE, 213–218. https://doi.org/10.1109/SIELMEN53755.2021.9600349

[30] Moumita Das, Xingyu Tao, and Jack C. P. Cheng. 2021. A Secure and Distributed Construction Document Management System Using Blockchain. In *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering*, Eduardo Toledo Santos and Sergio Scheer (Eds.). Lecture Notes in Civil Engineering, Vol. 98. Springer International Publishing, Cham, 850–862. https://doi.org/10.1007/978-3-030-51295-8_59

[31] Moumita Das, Xingyu Tao, Yuhan Liu, and Jack C.P. Cheng. 2022. A blockchain-based integrated document management framework for construction applications. *Automation in Construction* 133 (2022), 104001. https://doi.org/10.1016/j.autcon.2021.104001

[32] G. Deepika, V. Bharshini, and B. Kamala. 2022. A Reliable Integrated Storage And Management Using Blockchain. In *2022 1st International Conference on Computational Science and Technology (ICCST)*. IEEE, 863–867. https://doi.org/10.1109/ICCST55948.2022.10040333

[33] Amol Deshpande, Dayanand Ambawade, Hiten Bafna, Husain Challawala, and Jai Damani. 2023. Blockchain based Skill Verification System. In *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*. IEEE, 1588–1593. https://doi.org/10.1109/ICSCSS57650.2023.10169782

[34] Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali, and Robert Hierons. 20.03.2018 - 20.03.2018. Smart contracts vulnerabilities: a call for blockchain software engineering?. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 19–25. https://doi.org/10.1109/IWBOSE.2018.8327567

[35] Leonardo Dias Menezes, Luciano Vieira de Araújo, and Marislei Nishijima. 2023. Blockchain and smart contract architecture for notaries services under civil law: a Brazilian experience. *International journal of information security* (2023), 1–12. https://doi.org/10.1007/s10207-023-00673-3

[36] Ba-Lam Do, Hoang-Nam Dinh, Van-Thanh Nguyen, Manh-Hung Tran, Thanh-Long Le, and Viet-Thang Nghiem. 2022. B4E: A System for Creating and Validating Digital Credentials using Remote Signing and Blockchain. In *The 11th International Symposium on Information and Communication Technology*. ACM, New York, NY, USA, 420–426. https://doi.org/10.1145/3568562.3568656

[37] Naveen Kumar Dumpeti and Radhika Kavuri. 2021. WITHDRAWN: A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain. *Materials Today: Proceedings* (2021). https://doi.org/10.1016/j.matpr.2021.01.740

[38] Naveen Kumar Dumpeti and Radhika Kavuri. 2023. A Blockchain Based Decentralized Certificate Management System Using Hyperledger Fabric. In *Proceedings of the 14th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2022)*, Ajith Abraham, Thomas Hanne, Niketa Gandhi, Pooja Manghirmalani Mishra, Anu Bajaj, and Patrick Siarry (Eds.). Lecture Notes in Networks and Systems, Vol. 648. Springer Nature Switzerland, Cham, 474–484. https://doi.org/10.1007/978-3-031-27524-1_45

[39] Frank Ebbers and Murat Karaboga. 2021. Blockchain and Data Protection: An Evaluation of the Challenges and Solutions mentioned by German Stakeholders. In *Wirtschaftsinformatik 2021 Proceedings*, AIS eLibrary (Ed.).

[40] Alley El-Dorry, Mohamed Reda, Sherif Abd El Khalek, Shehab El-Din Mohamed, Radwa Mohamed, and Ayman Nabil. 2020. Egyptian Universities Digital Certificate Verification Model Using Blockchain. In *Proceedings of the 2020 9th International Conference on Software and Information Engineering (ICSIE)*. ACM, New York, NY, USA, 79–83. https://doi.org/10.1145/3436829.3436864

[41] Niloofar Etemadi, Yari Borbon-Galvez, Fernanda Strozzi, and Tahereh Etemadi. 2021. Supply Chain Disruption Risk Management with Blockchain: A Dynamic Literature Review. *Information* 12, 2 (2021), 70. https://doi.org/10.3390/info12020070

[42] Ghareeb Falazi, Uwe Breitenbücher, Frank Leymann, Stefan Schulte, and Vladimir Yussupov. 2023. Transactional Cross-Chain Smart Contract Invocations. *Distrib. Ledger Technol.* (aug 2023). https://doi.org/10.1145/3616023 Just Accepted.

[43] Efat Fathalla, Chonggang Wang, Xu Li, Robert Gazda, and Hongyi Wu. 2023. Redactable Distributed Ledgers: A Survey. *Distrib. Ledger Technol.* 2, 3, Article 24 (sep 2023), 26 pages. https://doi.org/10.1145/3596224

[44] Michèle Finck. 2019. *Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law?* Publications Office of the European Union, [Luxembourg].

[45] Gilbert Fridgen, Nikolas Guggenberger, Thomas Hoeren, Wolfgang Prinz, and Nils Urbach. 2019. Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik. https://www.bmvi.de/SharedDocs/DE/Artikel/DG/blockchain-grundgutachten.html

[46] Gilbert Fridgen, Florian Guggenmoos, Jannik Lockl, Alexander Rieger, Andre Schweizer, and Nils Urbach. 2018. Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process. https://doi.org/10.18420/BLOCKCHAIN2018{_}10

[47] Hrithik Gaikwad, Nevil D'Souza, Rajkumar Gupta, and Amiya Kumar Tripathy. 2021. A Blockchain-Based Verification System for Academic Certificates. In *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*. IEEE, 1–6. https://doi.org/10.1109/ICSCAN53069.2021.9526377

[48] Nata Goderdzishvili, Eka Gordadze, and Nikoloz Gagnidze. 2018. Georgia's Blockchain-powered Property Registration: Never blocked, Always Secured - Ownership Data Kept Best!. In *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, Atreyi Kankanhalli, Adegboyega Ojo, and Delfina Soares (Eds.). ACM, New York, NY, USA, 673–675. https://doi.org/10.1145/3209415.3209437

[49] Adeeba Habeeb, Vinod Kumar Shukla, Suchi Dubey, and Shaista Anwar. 2022. Blockchain Technology in Digital Certificate Authentication. In *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. IEEE, 1–5. https://doi.org/10.1109/ICRITO56286.2022.9964545

[50] Shinya Haga and Kazumasa Omote. 2022. Blockchain-Based Autonomous Notarization System Using National eID Card. *IEEE Access* 10 (2022), 87477–87489. https://doi.org/10.1109/ACCESS.2022.3199744

[51] Jongbeen Han, Heemin Kim, Hyeonsang Eom, and Yongseok Son. 2021. A decentralized document management system using blockchain and secret sharing. In *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, Chih-Cheng Hung, Jiman Hong, Alessio Bechini, and Eunjee Song (Eds.). ACM, New York, NY, USA, 305–308. https://doi.org/10.1145/3412841.3442077

[52] Timothy Harlian, Muhammad Faris Ruriawan, and Yudha Purwanto. 2022. Implementation of Blockchain for Digital Document Data Collection Website. In *2022 1st International Conference on Information System & Information Technology (ICISIT)*. IEEE, 425–430. https://doi.org/10.1109/ICISIT54091.2022.9873097

[53] M. M. Rakibul Hasan, Md. Mahinur Alam, and Kanita Jerin Tanha. 2022. Decentralized Blockchain Based Land Deed Verification and Reservation System in Bangladesh. In *2022 25th International Conference on Computer and Information Technology (ICCIT)*. IEEE, 971–975. https://doi.org/10.1109/ICCIT57492.2022.10054857

[54] Minhua He, Xu Han, Frank Jiang, Rongbai Zhang, Xingzi Liu, and Xiao Liu. 2020. BlockMeds: A Blockchain-Based Online Prescription System with Privacy Protection. In *Service-Oriented Computing – ICSOC 2019 Workshops*, Sami Yangui, Athman Bouguettaya, Xiao Xue, Noura Faci, Walid Gaaloul, Qi Yu, Zhangbing Zhou, Nathalie Hernandez, and Elisa Y. Nakagawa (Eds.). Lecture Notes in Computer Science, Vol. 12019. Springer International Publishing, Cham, 299–303. https://doi.org/10.1007/978-3-030-45989-5_27

[55] Andres Heredia and Gabriel Barros-Gavilanes. 2021. Dealing with multi-step verification processes for certification issuance in universities. In *Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, Luiz F. Bittencourt and Alan Sill (Eds.). ACM, New York, NY, USA, 1–5. https://doi.org/10.1145/3492323.3495622

[56] Ching-Sheng Hsu, Shu-Fen Tu, and Pei-Chia Chiu. 2022. Design of an e-diploma system based on consortium blockchain and facial recognition. *Education and Information Technologies* 27, 4 (2022), 5495–5519. https://doi.org/10.1007/s10639-021-10840-5

[57] Hsiao-Shan Huang, Tian-Sheuan Chang, and Jhih-Yi Wu. 2020. A Secure File Sharing System Based on IPFS and Blockchain. In *Proceedings of the 2020 2nd International Electronics Communication Conference*. ACM, New York, NY, USA, 96–100. https://doi.org/10.1145/3409934.3409948

[58] Joschka Andreas Hüllmann, Kariko Kimathi, and Pauline Weritz. 2024. Large-Scale Agile Project Management in Safety-Critical Industries: A Case Study on Challenges and Solutions. *Information Systems Management* (May 2024), 1–23. https://doi.org/10.1080/10580530.2024.2349886

[59] Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, and Shaikh Akib Shahriyar. 2021. DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, 1262–1267. https://doi.org/10.1109/ICICV50876.2021.9388428

[60] Sebastian-Vlad Ionescu. 2022. E-prescription using blockchain technology. In *2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health)*. IEEE, 1–7. https://doi.org/10.1109/SMARTBLOCK4HEALTH56071.2022.10034520

[61] Bagas Fadillah Islamay, Yudha Purwanto, and Muhammad Faris Ruriawan. 2022. Implementation of Blockchain and Peer-to-peer Network for Digital Document Management. In *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)*. IEEE, 1–6. https://doi.org/10.1109/ICACNIS57039.2022.10055538

[62] J. G. L. A. Jayasinghe, K. G. S. Shiranthaka, T. Kavith, M. H. D. V. Jayasinghe, Kavinga Yapa Abeywardena, and Kanishka Yapa. 2022. Blockchain-based Secure Environment for Electronic Health Records. In *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 1–6. https://doi.org/10.1109/ICCCNT54827.2022.9984371

[63] Thomas Jensen, Jonas Hedman, and Stefan Henningsson. 2019. How TradeLens Delivers Business Value With Blockchain Technology. *MIS Quarterly Executive* 18, 4 (2019), 221–243. https://doi.org/10.17705/2msqe.00018

[64] Branko Jovović, Tomo Popović, Stevan Šandi, and Zoran Djikanović. 2023. A Blockchain-Based Approach to Management of University Diploma Authenticity. In *2023 27th International Conference on Information Technology (IT)*. IEEE, 1–4. https://doi.org/10.1109/IT57431.2023.10078715

[65] Shaik Khaleelullah, Sai Teja Vangapalli, Malavika Gaddam, Vitesh Sai Hanumakonda, and Uday Kiran Goud Gangapuram. 2023. Verifcation of Academic Records Using Hyperledger Fabric and IPFS. In *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*. IEEE, 210–217. https://doi.org/10.1109/ICPCSN58827.2023.00040

[66] Shawal Khalid and Chris Brown. 2023. Software Engineering Approaches Adopted By Blockchain Developers. In *2023 Tenth International Conference on Software Defined Systems (SDS)*. IEEE, 1–6. https://doi.org/10.1109/SDS59856.2023.10329007

[67] Mansoor Khan, Oğuz Bayat, and Uğur Coruh. 2020. Performance Analysis of Blockchain-Based Systems for Industry Applications. In *Proceedings of the 6th International Conference on Engineering & MIS 2020*, Raisa Uskenbayeva, Yevgeniya Daineko, and Shadi A. Aljawarneh (Eds.). ACM, New York, NY, USA, 1–21. https://doi.org/10.1145/3410352.3410836

[68] Ashish Khanna, Devansh Singh, Ria Monga, Tarun Kumar, Ishaan Dhull, and Tariq Hussain Sheikh. 2023. Integration of Blockchain-Enabled SBT and QR Code Technology for Secure Verification of Digital Documents. In *Proceedings of Data Analytics and Management*, Abhishek Swaroop, Zdzislaw Polkowski, Sérgio Duarte Correia, and Bal Virdee (Eds.). Lecture Notes in Networks and Systems, Vol. 788. Springer Nature Singapore, Singapore, 293–302. https://doi.org/10.1007/978-981-99-6553-3_23

[69] Eu Wang Kim, Min Seo Park, Kyoungmin Kim, and Kyong Ju Kim. 2022. Blockchain-Based Automatic Tracking and Extracting Construction Document for Claim and Dispute Support. *KSCE Journal of Civil Engineering* 26, 9 (2022), 3707–3724. https://doi.org/10.1007/s12205-022-2181-z

[70] Barbara Kitchenham and Stuart Charters. 2007. Guidelines for performing Systematic Literature Reviews in Software Engineering. 2 (2007).

[71] Ioannis Koulizakis and Euripides Loukis. 2020. A development framework for blockchain technologies in digital government. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, Yannis Charalabidis, Maria Alexandra Cunha, and Demetrios Sarantis (Eds.). ACM, New York, NY, USA, 129–136. https://doi.org/10.1145/3428502.3428519

[72] Udo Kuckartz. 2014. *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software.* SAGE Publications Ltd.

[73] A. Vijaya Kumar, Ghanta Vyshnavi, Pendyala Harshini, and Papareddy Sushanth Reddy. 2022. A Blockchain-based Document Verification Model in Freshers Hiring Process. In *2022 6th International Conference on Electronics, Communication and Aerospace Technology*. IEEE, 776–781. https://doi.org/10.1109/ICECA55336.2022.10009358

[74] K. Kumutha and S. Jayalakshmi. 2021. Hyperledger Fabric Blockchain Framework: Efficient Solution for Academic Certificate Decentralized Repository. In *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. IEEE, 1584–1590. https://doi.org/10.1109/I-SMAC52330.2021.9640785

[75] K. Lalitha, L. Sowmiya, S. Sundareswari, and T. Srinithi. 2023. Digital Verification And Face Recognition. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 1–6. https://doi.org/10.1109/ICCCNT56998.2023.10308105

[76] Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, Artur Rösch, and Andrè Schweizer. 2023. Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry. In *Wirtschaftsinformatik*

2023 Proceedings, AIS eLibrary (Ed.). https://aisel.aisnet.org/wi2023/78

[77] Minh-Quan Le, Hai-Duong Le, Anh Vu Dinh-Duc, and Thanh-Tung Tran. 2023. IU-TransCert: A Blockchain-Based System for Academic Credentials with Auditability. In *Proceedings of the 12th International Symposium on Information and Communication Technology*. ACM, New York, NY, USA, 746–753. https://doi.org/10.1145/3628797.3628822

[78] Roger E. Levien. 1991. *The civilizing currency: documents and their revolutionary technologies.* MIT Press, Cambridge, MA, USA, 205–239.

[79] Zhongwen Li, Yang Wu, Zhenhui Tang, and Qiang Tang. 2023. Research and Implementation of Electronic Seal System Based on Blockchain Technology. In *2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*. IEEE, 28–32. https://doi.org/10.1109/ITAIC58329.2023.10408984

[80] Z. Li, Ray Y. Zhong, Z. G. Tian, Hong-Ning Dai, Ali Vatankhah Barenji, and George Q. Huang. 2021. Industrial Blockchain: A state-of-the-art Survey. *Robotics and Computer-Integrated Manufacturing* 70, 1 (2021), 102124. https://doi.org/10.1016/j.rcim.2021.102124

[81] Zoey Ziyi Li, Han Wang, Dragan Gasevic, Jiangshan Yu, and Joseph K. Liu. 2023. Enhancing Blockchain Adoption through Tailored Software Engineering: An Industrial-grounded Study in Education Credentialing. *Distrib. Ledger Technol.* 2, 4 (2023), 1–24. https://doi.org/10.1145/3632532

[82] Mohamed Litoussi, Mohamed Fartitchou, Khalid El Makkaoui, Abdellah Ezzati, and Zakaria El Allali. 2022. Digital Certifications in Moroccan Universities: Concepts, Challenges, and Solutions. *Procedia Computer Science* 201 (2022), 95–100. https://doi.org/10.1016/j.procs.2022.03.015

[83] Dan Liu. 2023. Research on Human Resource Management Information System Based on Big Data Blockchain Architecture. In *2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*. IEEE, 383–386. https://doi.org/10.1109/ICEIB57887.2023.10170684

[84] Haitham Mahmoud, Junaid Arshad, and Adel Aneiba. 2024. A Systematic Review of Blockchain-based Privacy-Preserving Reputation Systems for IoT Applications. *Distrib. Ledger Technol.* (jun 2024). https://doi.org/10.1145/3674156 Just Accepted.

[85] Christian Mahrt and Andreas Speck. 2021. Simple Anti-fraud Document Authentication Concept for Public Services. In *Human Centred Intelligent Systems*, Alfred Zimmermann, Robert J. Howlett, Lakhmi C. Jain, and Rainer Schmidt (Eds.). Smart Innovation, Systems and Technologies, Vol. 244. Springer Singapore, Singapore, 13–25. https://doi.org/10.1007/978-981-16-3264-8_2

[86] Giulia Maragno, Luca Gastaldi, Luca Tangi, and Michele Benedetti. 2021. Blockchain applications within the public sector: evidence from an international census. In *DG.O2021: The 22nd Annual International Conference on Digital Government Research*. ACM, New York, NY, USA, 479–488. https://doi.org/10.1145/3463677.3463699

[87] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli. 2020. ABCDE –agile block chain DApp engineering. *Blockchain: Research and Applications* 1, 1 (2020), 100002. https://doi.org/10.1016/j.bcra.2020.100002

[88] Dusica Marijan and Chhagan Lal. 2022. Blockchain verification and validation: Techniques, challenges, and research directions. *Computer Science Review* 45 (2022), 100492. https://doi.org/10.1016/j.cosrev.2022.100492

[89] Philipp Mayring. 2015. Qualitative Content Analysis: Theoretical Background and Procedures. In *Approaches to Qualitative Research in Mathematics Education*, Angelika Bikner-Ahsbahs, Christine Knipping, and Norma Presmeg (Eds.). Springer Netherlands, Dordrecht, 365–380. https://doi.org/10.1007/978-94-017-9181-6_13

[90] J. Meier and R. Sprague. 1996. Towards a better understanding of electronic document management. In *Proceedings of HICSS-29: 29th Hawaii International Conference on System Sciences*, Vol. 5. 53–61 vol.5. https://doi.org/10.1109/HICSS.1996.495298

[91] Neha Mishra and Haim Levkowitz. 2021. PDV: Permissioned Blockchain based Personal Data Vault using Predictive Prefetching. In *2021 3rd Blockchain and Internet of Things Conference*. ACM, New York, NY, USA, 59–69. https://doi.org/10.1145/3475992.3476001

[92] Roman Mühlberger, Stefan Bachhofner, Eduardo Castelló Ferrer, Claudio Di Ciccio, Ingo Weber, Maximilian Wöhrer, and Uwe Zdun. 2020. Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World. In *Business Process Management: Blockchain and Robotic Process Automation Forum*, Aleksandre Asatiani, José María García, Nina Helander, Andrés Jiménez-Ramírez, Agnes Koschmider, Jan Mendling, Giovanni Meroni, and Hajo A. Reijers (Eds.). Lecture Notes in Business Information Processing, Vol. 393. Springer International Publishing, Cham, 35–51. https://doi.org/10.1007/978-3-030-58779-6_3

[93] E. Mutharasan, J. Bharathi, K. Nithesh, S. Bose, D. Prabhu, and T. Anitha. 2023. Ethereum-Based Certificate Creation and Verification Using Blockchain. In *Futuristic Communication and Network Technologies*, N. Subhashini, Morris. A. G. Ezra, and Shien-Kuei Liaw (Eds.). Lecture Notes in Electrical Engineering, Vol. 966. Springer Nature Singapore, Singapore, 339–354. https://doi.org/10.1007/978-981-19-8338-2_28

[94] Md. Naimur Rahman, Rownak Kabir, Md. Abdul Hamid, and M. F. Mridha. 2021. IDPchain: Blockchain-Based International Driving Permit and Traffic Crime Reporting System. In *Emerging Technologies in Data Mining and Information Security*, Aboul Ella Hassanien, Siddhartha Bhattacharyya, Satyajit Chakrabati, Abhishek Bhattacharya, and Soumi Dutta (Eds.). Advances in Intelligent Systems and Computing, Vol. 1286. Springer Singapore, Singapore, 519–532. https://doi.org/10.1007/978-981-15-9927-9_50

[95] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

[96] Duc-Hiep Nguyen, Dinh-Nghia Nguyen-Duc, Nguyen Huynh-Tuong, and Hoang-Anh Pham. 2018. CVSS: A Blockchainized Certificate Verifying Support System. In *Proceedings of the Ninth International Symposium on Information and Communication Technology - SoICT*

2018, Unknown (Ed.). ACM Press, New York, New York, USA, 436–442. https://doi.org/10.1145/3287921.3287968

[97] G. D. Heshan Niranga, Vidya S. Nair, and Sai Shibu N. B. 2022. Design of a Secured Medical Data Access Management Using Ethereum Smart Contracts, Truffle Suite and Web3. In *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, Jeremy Gummeson, Sunghoon Ivan Lee, Jie Gao, and Guoliang Xing (Eds.). ACM, New York, NY, USA, 1215–1221. https://doi.org/10.1145/3560905.3568180

[98] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman. 2019. Decentralized document version control using ethereum blockchain and IPFS. *Computers & Electrical Engineering* 76 (2019), 183–197. https://doi.org/10.1016/j.compeleceng.2019.03.014

[99] Robert Norvill, Cyril Cassanges, Wazen Shbair, Jean Hilger, Andrea Cullen, and Radu State. 2020. A Security and Privacy Focused KYC Data Sharing Platform. In *BSCI '20*, Keke Gai, Kim-Kwang Raymond Choo, Jiamou Liu, and Kim-Kwang Raymond Choo (Eds.). The Association for Computing Machinery, New York, NY, 151–160. https://doi.org/10.1145/3384943.3409431

[100] Jørgen Svennevik Notland, Jakob Svennevik Notland, and Donn Morrison. 2020. The Minimum Hybrid Contract (MHC): Combining Legal and Blockchain Smart Contracts. In *Proceedings of the Evaluation and Assessment in Software Engineering*, Jingyue Li, Letizia Jaccheri, Torgeir Dingsøyr, and Ruzanna Chitchyan (Eds.). Association for Computing Machinery, [S.l.], 390–397. https://doi.org/10.1145/3383219.3383275

[101] Sae-Yong Oh, Sang-Hyun Cho, Sung-Hwa Han, and Gwang-Yong Gim. 2019. A Study on the Pre-verification of Data and the Implementation of Platform in Electronic Trade Using Blockchain. In *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. IEEE, 320–330. https://doi.org/10.1109/SNPD.2019.8935826

[102] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M. Lalu, Tianjing Li, Elizabeth W. Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas, Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher. 2021. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ (Clinical research ed.)* 372 (2021), n71. https://doi.org/10.1136/bmj.n71

[103] Kunal Pal and C. R. S. Kumar. 2021. QR Code Based Smart Document Implementation Using Blockchain and Digital Signature. In *Data Management, Analytics and Innovation*, Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas, and Jan Martinovic (Eds.). Advances in Intelligent Systems and Computing, Vol. 1174. Springer Singapore, Singapore, 449–465. https://doi.org/10.1007/978-981-15-5616-6_32

[104] Ari Pambudi, Suryari Purnama, Tsara Ayuninggati, Nuke Puji Lestari Santoso, and Anggun Oktariyani. 2021. Legality On Digital Document Using Blockchain Technology: An Exhaustive Study. In *2021 Sixth International Conference on Informatics and Computing (ICIC)*. IEEE, 1–6. https://doi.org/10.1109/ICIC54025.2021.9632860

[105] Konstantinos Papageorgiou and Georgios Spathoulas. 2022. Self-sovereign, verifiable, ubiquitous and privacy preserving public entity documents through the use of blockchain technology. In *2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 1–8. https://doi.org/10.1109/SEEDA-CECNSM57760.2022.9932938

[106] Guy Paré, Marie-Claude Trudel, Mirou Jaana, and Spyros Kitsiou. 2015. Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management* 52, 2 (2015), 183–199.

[107] Adrian Petcu, Madalin Frunzete, and Dan Alexandru Stoichescu. 2023. A Practical Implementation Of A Digital Document Signature System Using Blockchain. In *2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*. IEEE, 1–6. https://doi.org/10.1109/ATEE58038.2023.10108308

[108] Julien Polge, Jérémy Robert, and Yves Le Traon. 2020. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express* 59 (2020), 134. https://doi.org/10.1016/j.icte.2020.09.002

[109] Suporn Pongnumkul, Chanop Khonnasee, Swiss Lertpattanasak, and Chantri Polprasert. 03122020. Proof-of-Concept (PoC) of Land Mortgaging Process in Blockchain-based Land Registration System of Thailand. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*. ACM, New York, NY, USA, 100–104. https://doi.org/10.1145/3390566.3391669

[110] Andrea Ponza, Simone Scannapieco, Anna Simone, and Claudio Tomazzoli. 2020. Envisioning the Digital Transformation of Financial Documents: A Blockchain-Based Bill of Exchange. In *Blockchain and Applications*, Javier Prieto, António Pinto, Ashok Kumar Das, and Stefano Ferretti (Eds.). Advances in Intelligent Systems and Computing, Vol. 1238. Springer International Publishing, Cham, 81–90. https://doi.org/10.1007/978-3-030-52535-4_9

[111] Simone Porru, Andrea Pinna, Michele Marchesi, and Roberto Tonelli. 2017. Blockchain-Oriented Software Engineering: Challenges and New Directions. In *2017 IEEE/ACM 39th International Conference on Software Engineering companion*. IEEE, Piscataway, NJ, 169–171. https://doi.org/10.1109/ICSE-C.2017.142

[112] R. T. Prabu, S. Diwakaran, R. Hemalatha, V. Senthilkumar, Madhini. M, and B. Thiyaneswaran. 2023. A Novel Design of Secured BlockChain Assisted Land Registration Mechanism by using Enhanced Verification Principles. In *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*. IEEE, 1–9. https://doi.org/10.1109/RMKMATE59243.2023.10369546

[113] P. Pranav, A. H. Saikiran, M. M. Mukul, B. Ravishankar, and V. N. Shailaja. 2020. Critical Analysis of International Shipments within Mainstream Blockchain Framework using Industrial Engineering Techniques. In *2020 International Conference on Mainstreaming Block*

Chain Implementation (ICOMBI). IEEE, 1–9. https://doi.org/10.23919/ICOMBI48604.2020.9203429

[114] M. Dhulavvagol Praveen, S. G. Totad, Mahadev Rashinkar, Ribhav Ostwal, Suprita Patil, and Priyanka M. Hadapad. 2022. Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation. *Procedia Computer Science* 215 (2022), 370–379. https://doi.org/10.1016/j.procs.2022.12.039

[115] Hauke Precht and Jorge Marx Gómez. 2021. Towards GDPR Enforcing Blockchain Systems. In *Innovation Through Information Systems*, Frederik Ahlemann, Reinhard Schütte, and Stefan Stieglitz (Eds.). Lecture Notes in Information Systems and Organisation, Vol. 47. Springer International Publishing, Cham, 440–446. https://doi.org/10.1007/978-3-030-86797-3{_}29

[116] Christian Esteban Pulmano, Maria Regina Justina Esguerra Estuar, Marlene Mana de Leon, Lenard Paulo Velasco Tamayo, Abraham Tan Magpantay, Hans Calvin Lee Tan, and Nicole Allison Siy Co. 2023. CREDERE: A Modular Blockchain Implementation for the Issuance, Sharing, and Verification of Digital Credentials. In *2023 The 6th International Conference on Software Engineering and Information Management*. ACM, New York, NY, USA, 228–233. https://doi.org/10.1145/3584871.3584904

[117] Luyl-Da Quach, Tien Quang Huynh, Uy Hoang Anh Cao, Khoi Minh Nguyen, Khoa Dang Nguyen, Tu Xuan Le, and Phuoc_Hai Huynh. 2023. First approach to Digitalize Academic Records in Viet Nam using Blockchain Technology. In *Proceedings of the 2023 8th International Conference on Intelligent Information Technology*. ACM, New York, NY, USA, 86–91. https://doi.org/10.1145/3591569.3591583

[118] Divya Shree R, Keerthana G, KrisshneShri M, and Vasantha Kumar V. 2022. Digital Documents Verification System. In *2022 International Conference on Computer, Power and Communications (ICCPC)*. IEEE, 389–392. https://doi.org/10.1109/ICCPC55978.2022.10072252

[119] Tasfia Rahman, Sumaiya Islam Mouno, Arunangshu Mojumder Raatul, Abul Kalam Al Azad, and Nafees Mansoor. 2023. Verifi-Chain: A Credentials Verifier Using Blockchain and IPFS. In *Inventive Communication and Computational Technologies*, G. Ranganathan, George A. Papakostas, and Álvaro Rocha (Eds.). Lecture Notes in Networks and Systems, Vol. 757. Springer Nature Singapore, Singapore, 361–371. https://doi.org/10.1007/978-981-99-5166-6_24

[120] T.S.Raja Rajeswari, Sk Khaja Shareef, Sameer Khan, N. Venkatesh, Akhtar Ali, and V. Sri Monika Devi. 2021. Generating and Validating Certificates Using Blockchain. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 1048–1052. https://doi.org/10.1109/ICCES51350.2021.9489105

[121] Denis Rangelov, Nikolay Tcholtchev, Philipp Lammel, and Ina Schieferdecker. 2019. Experiences Designing a Multi-Tier Architecture for a Decentralized Blockchain Application in the Energy Domain. In *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 1–7. https://doi.org/10.1109/ICUMT48472.2019.8970836

[122] K. Ravi Kishore, G. Jyostna, Mahesh U. Patil, P. R. Lakshmi Eswari, and E. Magesh. 2021. Blockchain Based Proof of Existence (PoE) Application for Educational Certificate Verification. In *Communication Software and Networks*, Suresh Chandra Satapathy, Vikrant Bhateja, M. Ramakrishna Murty, Nguyen Gia Nhu, and Jayasri Kotti (Eds.). Lecture Notes in Networks and Systems, Vol. 134. Springer Singapore, Singapore, 575–586. https://doi.org/10.1007/978-981-15-5397-4_58

[123] Md. Suman Reza, Sujit Biswas, Abdullah Alghamdi, Mesfer Alrizq, Anupam Kumar Bairagi, and Mehedi Masud. 2021. ACC: Blockchain Based Trusted Management of Academic Credentials. In *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*. IEEE, 438–443. https://doi.org/10.1109/iSES52644.2021.00104

[124] Joshua D. Roberts, Joanna F. Defranco, and D. Richard Kuhn. 2023. Data Block Matrix and Hyperledger Implementation: Extending Distributed Ledger Technology for Privacy Requirements. *Distrib. Ledger Technol.* 2, 2, Article 16 (jun 2023), 11 pages. https://doi.org/10.1145/3585539

[125] Boriana Rukanova, Jolien Ubacht, Selinde van Engelenburg, Yao-Hua Tan, Marco Geurts, Maarten Sies, Marcel Molenhuis, and Micha Slegt. 2021. Realizing value from voluntary business-government information sharing through blockchain-enabled infrastructures: The case of importing tires to the Netherlands using TradeLens. In *DG.O2021: The 22nd Annual International Conference on Digital Government Research*. ACM, New York, NY, USA, 505–514. https://doi.org/10.1145/3463677.3463704

[126] Amal C. Saji, V. V. Nandakishore, Akshay Vijayan, and John Prakash Joseph. 2020. BCGV: Blockchain Enabled Certificate Generation, Verification and Storage. In *ICDSMLA 2019*, Amit Kumar, Marcin Paprzycki, and Vinit Kumar Gunjan (Eds.). Lecture Notes in Electrical Engineering, Vol. 601. Springer Singapore, Singapore, 349–355. https://doi.org/10.1007/978-981-15-1420-3_36

[127] Oiza Salau and Steve A. Adeshina. 2021. Secure Document Verification System Using Blockchain. In *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*. IEEE, 1–7. https://doi.org/10.1109/ICMEAS52683.2021.9739812

[128] Johnny Saldana. 2009. *The coding manual for qualitative reseachers*. SAGE Publications Ltd.

[129] Shikhar Sarang, Dhruv Rana, Smit Patel, Darshil Savaliya, Udai Pratap Rao, and Akhil Chaurasia. 2022. Document Management System Empowered by Effective Amalgam of Blockchain and IPFS. *Procedia Computer Science* 215 (2022), 340–349. https://doi.org/10.1016/j.procs.2022.12.036

[130] Jakob Schaerer and Torsten Braun. 2022. A Distributed Calibration Certificate Infrastructure. In *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 1–4. https://doi.org/10.1109/BRAINS55737.2022.9909437

[131] Pratima Sharma, Suyel Namasudra, Naveen Chilamkurti, Byung-Gyu Kim, and Ruben Gonzalez Crespo. 2023. Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM Transactions on Sensor Networks* 19, 3 (2023), 1–17. https://doi.org/10.1145/3577926

[132] Hankun Shi and Xuelin Wang. 2018. Research on the Development Path of Blockchain in Shipping Industry. In *Proceedings of the Asia-Pacific Conference on Intelligent Medical 2018 & International Conference on Transportation and Traffic Engineering 2018 on - APCIM & ICTTE 2018*, Unknown (Ed.). ACM Press, New York, New York, USA, 243–247. https://doi.org/10.1145/3321619.3321671

[133] Disha Shinde, Snehal Padekar, Siddharth Raut, Abdul Wasay, and S. S. Sambhare. 2019. Land Registry Using Blockchain - A Survey of existing systems and proposing a feasible solution. In *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. IEEE, 1–6. https://doi.org/10.1109/ICCUBEA47591.2019.9129289

[134] Roti Islam Shithy, Nur Mohammad, H.N.Ashiqur Ruhullah, S. M. Yeamin Oni, and Md.Al Amin. 2021. A Blockchain Based Land Registration and Ownership Management System for Bangladesh. In *2021 4th International Conference on Blockchain Technology and Applications*. ACM, New York, NY, USA, 94–100. https://doi.org/10.1145/3510487.3510501

[135] Anjali Singh, S. P.S. Chauhan, and Amit Kumar Goel. 2023. Blockchain Based Verification of Educational and Professional Certificates. In *2023 2nd International Conference on Computational Systems and Communication (ICCSC)*. IEEE, 1–7. https://doi.org/10.1109/ICCSC56913.2023.10143008

[136] Heather A Smith and James D McKeen. 2003. Developments in practice VIII: Enterprise content management. *The Communications of the Association for Information Systems* 11, 1 (2003), 41.

[137] Pranshu Sood, Parikshit Palsania, Shivang Ahuja, Shivam Kumar, Kiran Khatter, and Atul Mishra. 2022. Decentralised & Collaborative DocuPad Using Blockchain. In *2022 IEEE Delhi Section Conference (DELCON)*. IEEE, 1–8. https://doi.org/10.1109/DELCON54057.2022.9752853

[138] Ralph H. Sprague. 1995. Electronic document management: challenges and opportunities for information systems managers. *MIS Q.* 19, 1 (mar 1995), 29–49. https://doi.org/10.2307/249710

[139] J. Timothy Sprehe. 2005. The positive benefits of electronic records management in the context of enterprise content management. *Government Information Quarterly* 22, 2 (Jan. 2005), 297–303. https://doi.org/10.1016/j.giq.2005.02.003

[140] Mircea Cristian Stana, Nicolae Goga, Constantin Viorel Marian, Ramona Popa, Catalina-Mihaela Vulpe, and Cristian Taslitchi. 2021. G-Cloud Briefcase - Electronic Archive for Academic Certificates and General Certificates of Education Documents Using Public Private Hyperspace for E-Government Library Services Based on NOSQL Databases. In *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, 1–5. https://doi.org/10.1109/BlackSeaCom52164.2021.9527826

[141] Miroslav Stefanovic, Dorde Przulj, Sonja Ristic, Darko Stefanovic, and Danilo Nikolic. 2022. Smart Contract Application for Managing Land Administration System Transactions. *IEEE Access* 10 (2022), 39154–39176. https://doi.org/10.1109/ACCESS.2022.3164444

[142] Ali Sunyaev. 2020. Distributed Ledger Technology. In *Internet Computing*, Ali Sunyaev (Ed.). Vol. 2. Springer International Publishing, Cham, 265–299. https://doi.org/10.1007/978-3-030-34957-8_9

[143] Ahmed Taha and Ahmed Zakaria. 2020?. Truver: a blockchain for verifying credentials: poster. In *The 35th Annual ACM Symposium on Applied Computing*, Chih-Cheng Hung, Tomas Cerny, Dongwan Shin, and Alessio Bechini (Eds.). Association for Computing Machinery, [New York, New York], 346–348. https://doi.org/10.1145/3341105.3374067

[144] Attoumane Tahar, Gervais Mendy, and Samuel Ouya. 2022. A Proof of Concept of the integration of blockchain with an ISO 19152:2012 based Land Administration System. In *Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications*. ACM, New York, NY, USA, 88–94. https://doi.org/10.1145/3581971.3581984

[145] Jing Tang, Tao Jia, Haibo Chen, and Chuncheng Wei. 2020. Research on Big Data Storage Method based on IPFS and Blockchain. In *2020 2nd International Conference on Video, Signal and Image Processing*. ACM, New York, NY, USA, 55–60. https://doi.org/10.1145/3442705.3442714

[146] Fatemeh Esmaeilnezhad Tanha, Aliakbar Hasani, Saqib Hakak, and Thippa Reddy Gadekallu. 2022. Blockchain-based cyber physical systems: Comprehensive model for challenge assessment. *Computers & Electrical Engineering* 103 (2022), 108347. https://doi.org/10.1016/j.compeleceng.2022.108347

[147] Rewat Thapa, Pankajeshwara Sharma, Joschka Andreas Hüllmann, and Bastin Tony Roy Savarimuthu. 2021. Identifying influence mechanisms in permissionless blockchain communities: The bitcoin case. In *42nd International Conference on Information Systems (ICIS)*. 1–17.

[148] Kentaroh Toyoda, Justin Lim Kim Moh, Nang Hsu Hlaing Mon, and Alvin Soo. 2022. Design and Implementation of Blockchain-enabled Immutable and Interoperable Data Management System for Enterprise Systems. In *2022 5th International Conference on Computers in Management and Business (ICCMB)*. ACM, New York, NY, USA, 7–11. https://doi.org/10.1145/3512676.3512678

[149] Horst Treiblmaier. 2020. Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. In *Blockchain and Distributed Ledger Technology Use Cases*, Horst Treiblmaier and Trevor Clohessy (Eds.). Progress in IS, Vol. 24. Springer International Publishing, Cham, 1–31. https://doi.org/10.1007/978-3-030-44337-5_1

[150] Horst Treiblmaier and Trevor Clohessy (Eds.). 2020. *Blockchain and Distributed Ledger Technology Use Cases*. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-44337-5

[151] Pooja Vairagkar and Sayli Patil. 2021. Digital Locker System for College or University Admissions Using Blockchain Technology. In *Data Management, Analytics and Innovation*, Neha Sharma, Amlan Chakrabarti, Valentina Emilia Balas, and Alfred M. Bruckstein (Eds.). Lecture Notes on Data Engineering and Communications Technologies, Vol. 70. Springer Singapore, Singapore, 353–366.

https://doi.org/10.1007/978-981-16-2934-1_23

[152] Mohit Vashistha and Ferdous Ahmed Barbhuiya. 2020. Document Management System using Blockchain and Inter Planetary File System. In *BSCI '20*, Keke Gai, Kim-Kwang Raymond Choo, Jiamou Liu, and Kim-Kwang Raymond Choo (Eds.). The Association for Computing Machinery, New York, NY, 212–213. https://doi.org/10.1145/3384943.3409443

[153] Garima Verma and Soumen Kanrar. 2024. Secure document sharing model based on blockchain technology and attribute-based encryption. *Multimedia Tools and Applications* 83, 6 (2024), 16377–16394. https://doi.org/10.1007/s11042-023-16186-z

[154] Fernando Vidal, Feliz Gouveia, and Christophe Soares. 2019. Analysis of Blockchain Technology for Higher Education. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, 28–33. https://doi.org/10.1109/CyberC.2019.00015

[155] Jan vom Brocke, Alexander Simons, Andrea Herbst, René Derungs, and Stefan Novotny. 2011. The business drivers behind ECM initiatives: a process perspective. *Business Process Management Journal* 17, 6 (Nov. 2011), 965–985. https://doi.org/10.1108/14637151111182710

[156] Jan vom Brocke, Alexander Simons, Björn Niehaves, Kai Riemer, Ralf Plattfaut, and Anne Cleven. 2009. Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In *Proceedings of the 17^{th} European Conference on Information Systems*, S. Newell, E. A. Whitley, N. Pouloudi, J. Wareham, and L. Mathiassen (Eds.). AIS eLibrary, United States, 2206–2217. http://aisel.aisnet.org/ecis2009/161/ Publication status: Published.

[157] Jan vom Brocke, Alexander Simons, Kai Riemer, Björn Niehaves, Ralf Plattfaut, and Anne Cleven. 2015. Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems* 37 (2015). https://doi.org/10.17705/1CAIS.03709

[158] Ziyuan Wang, Dain Yap Liffman, Dileban Karunamoorthy, and Ermyas Abebe. 2018. Distributed Ledger Technology for Document and Workflow Management in Trade and Logistics. In *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, Alfredo Cuzzocrea, James Allan, Norman Paton, Divesh Srivastava, Rakesh Agrawal, Andrei Broder, Mohammed Zaki, Selcuk Candan, Alexandros Labrinidis, Assaf Schuster, and Haixun Wang (Eds.). ACM, New York, NY, USA, 1895–1898. https://doi.org/10.1145/3269206.3269222

[159] Leena Wanganoo, Biranchi Prasad Panda, Rajesh Tripathi, and Vinod Kumar Shukla. 2021. Harnessing Smart Integration: Blockchain-Enabled B2C Reverse Supply Chain. In *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 261–266. https://doi.org/10.1109/ICCIKE51210.2021.9410677

[160] Jane Webster and Richard T. Watson. 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q* 26, 2 (2002), xiii–xxiii. http://dl.acm.org/citation.cfm?id=2017160.2017162

[161] Florian Wessling and Volker Gruhn. 30.04.2018 - 04.05.2018. Engineering Software Architectures of Blockchain-Oriented Applications. In *2018 IEEE International Conference on Software Architecture Companion (ICSA-C)*. IEEE, 45–46. https://doi.org/10.1109/ICSA-C.2018.00019

[162] Erik Westphal, Benjamin Leiding, and Hermann Seitz. 2023. Blockchain-based quality management for a digital additive manufacturing part record. *Journal of Industrial Information Integration* 35 (2023), 100517. https://doi.org/10.1016/j.jii.2023.100517

[163] Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, Dongxi Liu, Fengkie Junis, and Dony Ariadi Suwarsono. 2019. Designing Smart Contract for Electronic Document Taxation. In *Cryptology and Network Security*, Yi Mu, Robert H. Deng, and Xinyi Huang (Eds.). Lecture Notes in Computer Science, Vol. 11829. Springer International Publishing, Cham, 199–213. https://doi.org/10.1007/978-3-030-31578-8_11

[164] Dezhi Wu, Peng Shi, Liang Xu, and Hao Wang. 2020. A Document Processing Scheme for Journal Submissions Based on Locality Sensitive Hashing and Scale-invariant Feature Transform. In *2020 13th International Symposium on Computational Intelligence and Design (ISCID)*. IEEE, 282–285. https://doi.org/10.1109/ISCID51228.2020.00069

[165] Huiqun Wu, Yujuan Shang, Lei Wang, Lili Shi, Kui Jiang, and Jiancheng Dong. 2019. A Patient-Centric Interoperable Framework for Health Information Exchange via Blockchain. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. ACM, New York, NY, USA, 76–80. https://doi.org/10.1145/3376044.3376055

[166] Xiwei Xu, Cesare Pautasso, Liming Zhu, Qinghua Lu, and Ingo Weber. 2018. A Pattern Collection for Blockchain-based Applications. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs* (Irsee, Germany) *(EuroPLoP '18)*. Association for Computing Machinery, New York, NY, USA, Article 3, 20 pages. https://doi.org/10.1145/3282308.3282312

[167] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. 2017. A Taxonomy of Blockchain-Based Systems for Architecture Design. In *ICSA 2017*. IEEE, Piscataway, NJ, 243–252. https://doi.org/10.1109/ICSA.2017.33

[168] Sixin Xue, Xu Zhao, Xin Li, Guigang Zhang, and Chunxiao Xing. 2019. A Trusted System Framework for Electronic Records Management Based on Blockchain. In *Web Information Systems and Applications*, Weiwei Ni, Xin Wang, Wei Song, and Yukun Li (Eds.). Lecture Notes in Computer Science, Vol. 11817. Springer International Publishing, Cham, 548–559. https://doi.org/10.1007/978-3-030-30952-7_55

[169] Amrendra Singh Yadav, Nikita Singh, and Dharmender Singh Kushwaha. 2022. Sidechain: storage land registry data using blockchain improve performance of search records. *Cluster computing* 25, 2 (2022), 1475–1495. https://doi.org/10.1007/s10586-022-03535-0

[170] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. [n. d.]. Blockchain Technology Overview. https://doi.org/10.6028/NIST.IR.8202

[171] Mahmoud Abdulaziz Elsayed Yousef. 2023. Developing and Implementing Blockchain Identity Management to Verify Students' Certifications and Data (VeriOn). In *Proceedings of the Future Technologies Conference (FTC) 2022, Volume 2*, Kohei Arai (Ed.). Lecture Notes in Networks and Systems, Vol. 560. Springer International Publishing, Cham, 16–35. https://doi.org/10.1007/978-3-031-18458-1_2

[172] Chao Yuan, Mixue Xu, Xueming Si, and Bin Li. 2017. Blockchain with Accountable CP-ABE: How to Effectively Protect the Electronic Documents. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 800–803. https://doi.org/10.1109/ICPADS.2017.00111

[173] Liang Zhang, Haibin Kan, and Honglan Huang. 2022. Patient-centered cross-enterprise document sharing and dynamic consent framework using consortium blockchain and ciphertext-policy attribute-based encryption. In *Proceedings of the 19th ACM International Conference on Computing Frontiers*, Luca Sterpone, Andrea Bartolini, and Anastasiia Butko (Eds.). ACM, New York, NY, USA, 58–66. https://doi.org/10.1145/3528416.3530228

[174] Zixi Zhang. 2022. Blockchain Technology in Logistics. In *The 2022 4th International Conference on Blockchain Technology*. ACM, New York, NY, USA, 156–159. https://doi.org/10.1145/3532640.3532662

[175] Xingyan Zhao, Zhi Zhang, Renchuan Hu, Junyong Liu, Xiaodong Yang, Rui Zhang, and Hongjun Gao. 2022. Blockchain Technology Based Digital Document Management System Design. In *2022 7th Asia Conference on Power and Electrical Engineering (ACPEE)*. IEEE, 440–446. https://doi.org/10.1109/ACPEE53904.2022.9783819

[176] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[177] Rui Zhou, Kangan Shu, Dejun Xiang, Hang Sun, and Yang Liu. 2022. A Blockchain-based Electricity Retail Contracts Management System. In *Proceedings of the 2022 4th Blockchain and Internet of Things Conference*. ACM, New York, NY, USA, 46–53. https://doi.org/10.1145/3559795.3559802

[178] Valentin Zieglmeier, Gabriel Loyola Daiqui, and Alexander Pretschner. 2023. Decentralized Inverse Transparency with Blockchain. *Distrib. Ledger Technol.* 2, 3, Article 17 (sep 2023), 28 pages. https://doi.org/10.1145/3592624

A EXPLANATIONS OF THE REFERENCED ARTICLES

Table 14. Overview of analyzed studies

ID	Explanation
Legend: The coding categories of the articles are highlighted in *cursive*. The superscript T indicates the respective table of the category.	
[165]	The authors describe an *Ethereum*[T10]-based system that enables secure, tamper-proof sharing of electronic *health records*[T11]. They designed and *prototyped*[T12] a cross-enterprise document sharing blockchain framework, utilizing a *proxy*[T4]-based architecture, aiming to integrate different healthcare providers leveraging *off-chain and cloud storage*[T9]. Deriving from their provided description of the system, they implicitly leverage a *inbound-push*[T5] oracle further providing a *functional description*[T7] while not providing insights into SC *testing*[T6] or software engineering *methodology*[T8].
[148]	This study presents an *Ethereum*[T10]-based *off-chain*[T9] data storage system that is enterprise systems agnostic, aiming for a *general applicability*[T11]. With their systems, they aim to enable secure and immutable data sharing across organizations, demonstrating their approach with a *prototype*[T12] managing digital construction contracts. Based on their presented system architecture, it becomes apparent that they deploy a *proxy*[T4]-based architecture while implementing an *implicit inbound-push*[T5] oracle approach. No software engineering *methodology* [T8] is named. A *functional description*[T7] for SCs is offered but no SC *testing*[T6].
[57]	The authors present a file sharing system utilizing *IPFS*[T9] and blockchain for *general usage*[T11]. They focus on distributed access control and group key management utilizing an IPFS proxy to overcome existing limitations in similar systems. Based on their system overview *proposal*[T12], they employ a *proxy*[T4]-based architecture while being *blockchain agnostic*[T10]. Their proposed storage system relies on an *off-chain IPFS*[T9] approach alongside an *implicit use of inbound-push*[T5] oracles. Given the state of their proposal, the study neither includes SC *descriptions*[T7] nor insights into SC *testing*[T6] or any *software engineering methodology*[T8].

Continued on next page

ID	Description
[24]	Paper [24] presents a privacy-focused method for document management of *miscellaneous*[T11] nature and content. The authors emphasize the importance of protecting personal user data and focuses on a private/permissioned *Hyperledger Fabric*[T10] blockchain, enhanced with homomorphic encryption. The paper provides *explicit performance testing*[T6] insights of the *pilot*[T12] with *functional descriptions*[T7] of the used SCs. In the system, data is stored *off-chain within IPFS*[T9] including an *implicit*[T5] oracle pattern in a *proxy*[T4]-based architecture. The system is presented without any mentions of *software engineering methodologies*[T8].
[5]	Alniamy and Taylor [5] showcase a *Hyperledger Fabric*[T10]-based system for *general*[T11] sharing of data and scholarly studies. With the combination of Hyperledger Fabric and attribute-based encryption, they design an architecture aiming to achieve fine-grained access control and the possibility of data-sharing in a decentralized system. In their *prototype*[T12], the data is stored *off-chain along with cloud storage*[T9] and an *implicit inbound-push*[T5] oracle is used. The general system is classified as a *proxy*[T4]-based architecture. The needed SCs are described on a *functional*[T7] level without insights into possible SC *testing*[T6] or the used *software engineering methodology*[T8].
[25]	In this study, the authors discuss an *Ethereum*[T10]-based *prototype*[T12] system named GovChain that allows for *general*[T11] e-document management using *off-chain and IPFS*[T9] storage. To achieve authenticity, confidentiality, and proper representation of ownership, the authors focus on the adoption of ciphertext-policy attribute-based encryption, aiming for a trusted identity environment. The latter leads to a dedicated component within the architecture, making it a *proxy*[T4]-based approach. Developed SCs are presented with *code snippets*[T7] which underwent *explicit security testing*[T6]. Derived from the presented system and SCs, it uses the *implicitly inbound-push*[T5] oracle pattern. Even though the architecture and SCs are described in detail, no explicit *software engineering methodology*[T8] is mentioned.
[48]	The authors present a *pilot*[T12] study that leverages the *Bitcoin*[T10] blockchain to store the hash value of a digital *property*[T11] title document on-chain while the actual data is stored *off-chain in a relational database*[T9]. Derived from the system description, it leverages an *implicit*[T5] oracle pattern within a *proxy*[T4]-based architecture. Due to the lack of SC capabilities in the Bitcoin blockchain, the paper does not provide *SC descriptions*[T7] or *SC testing patterns*[T6]. Even though the presented system is in a pilot stage, a *software engineering methodology* [T8] is not mentioned.

Continued on next page

ID	Description
[99]	The *Ethereum*[T10]-based *prototype*[T12] presented in [99] aims to ease the process of *miscellaneous*[T11] document sharing in the context of know-your-customer compliance in- and between banks. The authors emphasize the necessity of privacy and security-enhancing approaches within the system. They employ an *off-chain storage with a relational database*[T9], thus use the oracle pattern *implicitly*[T5]. Required SCs are described on a *functional*[T7] level where *performance testing is implicitly*[T6] mentioned. Given that the systems architecture incorporates a dedicated access control component sitting in between applications and the blockchain component, the overall architecture is classified as *proxy*[T4]-based. The authors do not mention any *software engineering methodology* [T8].
[158]	This study presents a *Hyperledger Fabric*[T10]-based system for document management in the *logistics*[T11] domain. The authors developed a *proxy*[T4]-based architecture, implemented a *prototype*[T12], and provided a *functional description*[T7] for SCs but did not detail any SC *testing*[T6]. They use *on-chain*[T9] storage for the documents and *implicitly*[T5] make use of oracle patterns. No insights into a *software engineering methodology* [T8] for the development of their system is given.
[91]	In their paper, Mishra and Levkowitz [91] developed a *prototype*[T12] of a personal data vault based on *Hyperledger Iroha*[T10], aiming to enable users to store digital *personal documents*[T11] in a secure way. The study does not depict SCs in detail but presents SCs via *functional descriptions*[T7]. Aspects related to SC *testing*[T6] or a *software engineering methodology*[T8] are not mentioned. Based on the presented system and process flows, it is derived that a *proxy*[T4]-based architecture is developed that uses *implicit*[T5] oracle patterns. The document data of the personal data vault is stored *off-chain in cloud storage*[T9].
[125]	The case study by Rukanova et al. [125] analyzes the applicability of the TradeLense Platform as a *product*[T12], built on *Hyperledger Fabric*[T10], to support the *logistics*[T11] of importing tires to the Netherlands. The described system employs a *proxy*[T4]-based architecture but does not provide insights into the used *SCs*[T7] and their *testing*[T6] nor into the used *software engineering methodology*[T8]. However, it can be derived that the system *implicitly*[T5] uses oracle patterns alongside its *off-chain cloud storage*[T9].
[134]	The authors present a novel solution for *land registration and management*[T11] based on the *Hyperledger Fabric*[T10] blockchain. Their *prototype*[T12] leverages a *proxy*[T4]-based architecture. A dedicated client-server component is built for end users, allowing buyers and sellers to interact on the Hyperledger Fabric blockchain network. Derived from the presented *functional description*[T7] of developed SCs, the system uses *the inbound-push*[T5] oracle pattern implicitly but does not offer any details of SC *testing*[T6]. Data is stored *off-chain in relational databases*[T9]. No insights into a *software engineering methodology*[T8] is given.

Continued on next page

ID	Description
[175]	This paper presents a system design for digital document management *prototype*[T12] based on *Hyperledger Fabric*[T10]. The authors aim to digitize documents in the *construction*[T11] domain. The documents are stored *off-chain in IPFS*[T9], *implicitly employing oracle patterns*[T5]. The developed SCs are presented as *functional descriptions*[T7] but lack insights into potential SC *testing*[T6]. The developed system is *proxy*[T4]-based as the authors developed a dedicated middleware between the application and blockchain layer. No insights are given into the *software engineering methodology* [T8] used.
[104]	Pambudi et al. [104] present a *prototype*[T12] based on the *Ethereum*[T10] blockchain to tackle issues such as fraud and forgery of *academic certificates*[T11] in Indonesia. The developed architecture encompasses an *off-chain layer using IPFS*[T9] between user interactions and the blockchain, meaning it is categorized as a *proxy*[T4]-based architecture. Derived from the *functional description*[T7] of the used SCs the *inbound-push oracle pattern is implicitly*[T5] used. No insight are given about SC *testing*[T6] or a *software engineering methodology*[T8] .
[154]	To improve the authenticity and verification processes of *academic certificates*[T11], this paper presents a *blockchain agnostic*[T10] *prototype*[T12] using Blockcerts in the context of the University Fernando Pessoa. The architecture makes use of middleware components to interact with the blockchain layer on behalf of the user, making it a *proxy*[T4]-based architecture. Academic certificates are stored *off-chain in a digital wallet*[T9]. Used SCs are described on a *functional level*[T7] indicating an *implicit use of the oracle pattern*[T5] but without naming potential SC *testing*[T6] patterns. No insight into a *software engineering methodology* [T8] is given.
[127]	In this study, the authors do not rely on existing *blockchains*[T10] but developed a *prototype*[T12] from scratch for *general applicability*[T11] for the secure and forgery-resistant storage for electronic documents. Despite developing the system from scratch, the authors do not mention any used *software engineering methodology*[T8]. However, they provide *pseudo code and diagrams*[T7] for the SCs and the system but they do not detail any SC *testing*[T6]. Derived from the presented system, they make use of a *proxy*[T4]-based architecture where documents and data are stored *off-chain in IPFS*[T9] along with an *implicit oracle pattern*[T5].
[47]	The paper presented by Gaikwad et al. [47] proposes a *Ethereum*[T10]-based *prototype*[T12] to deal with creation and verification of digital *academic certificates*[T11]. They developed a *proxy*[T4]-based architecture as they make use of a web-application laying between the user and the blockchain network. Developed SCs are *functionally described*[T7] without mentioning SC *testing*[T6] approaches. Derived from their description, the authors *implicitly use the oracle pattern*[T5]. No insight is given how documents are *stored*[T9]. No *software engineering methodology*[T8] is mentioned.

Continued on next page

ID	Description
[74]	By developing a *Hyperledger Fabric*[T10]-based blockchain system *prototype*[T12] for the management and verification of *academic certificates*[T11], Kumutha and Jayalakshmi [74] aim to overcome existing problems related to time-consuming certificate verification. The data of the academic certificates is stored *off-chain in a NoSQL database*[T9] leading to the *implicit usage of the oracle pattern*[T5]. They developed a web application for the user that interacts on their behalf with the blockchain layer, making it a *proxy*[T4]-based architecture. The used SCs are presented as a *functional description*[T7] without naming SC *testing*[T6] patterns. No insight into an employed *software engineering methodology*[T8] is given.
[137]	The authors presented a *prototype*[T12] based on *Blockstack*[T10] aiming for a *general applicability*[T11] in terms of managing documents as a decentralized and collaborative DocuPad. They use *GAIA as off-chain storage*[T9] to store the document data, *implicitly using the oracle pattern*[T5] within a *proxy*[T4]-based architecture. Developed SCs are presented via *functional description*[T7] without explaining SC *testing*[T6] or a used *software engineering methodology*[T8].
[141]	To overcome potential data tampering issues in long time storage and correctness of *land administration*[T11] records, Stefanovic et al. [141] *prototyped*[T12] an *Ethereum*[T10]-based system. They present *code*[T7] of the developed SC and *explicitly mention the inbound-push*[T5] oracle pattern as well as *explicitly describe performance testing*[T6] of the developed SC. Their overall architecture is *proxy*[T4]-based along with *off-chain in relational databases*[T9]. Even though their method is described in detail, they do not mention any specific *software engineering methodology*[T8].
[123]	In this study, a *prototype*[T12] of the Academic Credentials Chain based on *Hyperledger Fabric*[T10] is presented to enable secure management and sharing of *academic certificates*[T11]. The authors include a management server that interacts on behalf of the user with the blockchain network, making it a *proxy*[T4]-based architecture. *Off-chain storage with relational database*[T9] is utilized leading to an *implicit oracle pattern*[T5]. Developed SCs are presented via *functional description*[T7] without discussing SC *testing patterns*[T6] or a used *software engineering methodology*[T8].
[50]	In this paper, Haga and Omote [50] design and implement a *prototype*[T12] based on the *Ethereum*[T10] blockchain to enable fixed data notarization for *general*[T11] documents. Their architecture makes use of a web application sitting between clients/users and the blockchain network, making it a *proxy*[T4]-based system. The developed SCs are described *functionally*[T7] but do not mention SC *testing patterns*[T6]. Based on their presented design and architecture, the *implicit usage of the oracle pattern*[T5] is derived. It is *unclear*[T9] if on-chain or off-chain storage is utilized. They note that only a hash value of the document is stored on-chain. The actual document storage seems to be out of scope. No insight into an employed *software engineering methodology*[T8] is given.

Continued on next page

ID	Description
[168]	The paper presented by Xue et al. [168] proposes the use of the *Ethereum*^{T10} blockchain to develop a *prototype*^{T12} for managing *general*^{T11} electronic records and documents to ensure trustworthy, credible and authentic record management. They designed a *proxy*^{T4}-based system *implicitly using the oracle pattern*^{T5} and designed *off-chain storage in relational databases*^{T9}. The developed SCs are presented via *functional description*^{T7}, not mentioning SC *testing*^{T6} patterns. No *software engineering methodology*^{T8} is mentioned in the paper.
[12]	Bandara et al. [12] present Lekana, a *prototype*^{T12} based on the *Mystiko*^{T10} blockchain to build an archive storage system, using the example of *e-invoices*^{T11}. The goal is to enhance existing systems with blockchain benefits such as immutability, privacy, and ownership management. In their study, they *do not*^{T7} explicitly mention SC functional descriptions but *implicitly refer to performance testing*^{T6}. Their overall architecture follows the *proxy*^{T4}-based approach with *off-chain storage in NoSQL databases*^{T9}, only storing the document hashes on-chain. Hence, they *make use of the oracle pattern implicitly*^{T5}. There is no reference to a *software engineering methodology*^{T8}.
[19]	In this paper, the authors describe the usage of the SPROOF platform to enable management of *general*^{T11} digital documents with attribute-based authentication to overcome paper-based limitations such as loss or counterfeits. They developed a *prototype*^{T12} based on the *Ethereum*^{T10} blockchain in combination with *off-chain storage in IPFS*^{T9}. The developed SC is presented as *code*^{T7} and indicated *implicit usage of the oracle pattern*^{T5} but without mentioning SC *testing*^{T6} patterns or a used *software engineering methodology*^{T8}. Their system is categorized as *proxy*^{T4}-based.
[54]	This study presets BlockMeds which is a *prototype*^{T12} based on the *Hyperledger Fabric*^{T10} blockchain aimed to foster privacy in the *healthcare*^{T11} by enabling digital prescriptions. The authors developed a *proxy*^{T4}-based architecture and provide a *functional description*^{T7} of the developed SCs, not naming any SC *testing*^{T6} patterns or a used *software engineering methodology*^{T8}. They use *off-chain storage with relational databases*^{T9} and *implicitly use the oracle pattern*^{T5}.
[30]	In order to ensure confidentiality and enhance the integrity of *construction*^{T11} documents, Das et al. [30] developed a *prototype*^{T12} based on *Ethereum*^{T10}. The developed SCs are presented in form of several *diagrams*^{T7} but without naming potential SC *testing patterns*^{T6}. Overall, the architecture is *dApp*^{T4}-based as the user directly interacts with the SCs. The system uses *off-chain storage with IPFS*^{T9}, *implicitly using the oracle pattern*^{T5}. There is no employed *software engineering methodology*^{T8} mentioned in the paper.

Continued on next page

ID	Description
[122]	In their study, Ravi Kishore et al. [122] *prototyped*[T12] a system that enables the verification of authenticity of *academic certificates*[T11] using *Hyperledger Fabric*[T10]. The goal is the optimization of existing verification processes leveraging blockchain property such as immutability, transparency and authenticity. Their proposed architecture envisions a REST API between the application for end users and the SC and blockchain level meaning it is designed as a *proxy*[T4]-based architecture. While the SCs are *not described*[T7] in greater detail, the presented measurements reveals *implicit performance testing*[T6] of SC. To store actual data and documents, *off-chain storage with IPFS*[T9] is used along with an *implicit use of the oracle pattern*[T5]. The authors do not mention any potentially used *software engineering methodology*[T8].
[94]	In order to provide a tamper-proof and easy to verify international driving permit as a digital *personal documents*[T11], the authors developed a *prototype*[T12] leveraging *Hyperledger Fabric*[T10] along with *on-chain*[T9] storage. They present a *proxy*[T4]-based architecture with *functional descriptions*[T7] of SCs from which an *implicit usage of the oracle pattern*[T5] is derived. The study does not grant insight into SC *testing*[T6] or employed *software engineering methodologies*[T8].
[110]	The authors present a *proposal*[T12] to use *blockchain*[T10] as an enabler for digital Bills of Exchange used in *shipment*[T11], ensuring confidentiality, tamper-resistance and legal validity. In their proposal, they argue for *off-chain storage with relational databases*[T9] and a *proxy*[T4]-based architecture, *implicitly describing the oracle pattern*[T5]. They provide *functional descriptions*[T7] of needed the SCs but do not detail any SC *testing patterns*[T6] or *software engineering methodologies*[T8].
[31]	This paper presents a *Hyperledger Fabric*[T10]-based *prototype*[T12] for managing *construction*[T11]-related documents, enabling approval workflows while ensuring document authenticity and tamper-resistance. The developed architecture is *dApp*[T4]-based, uses *off-chain storage with IPFS*[T9] and uses *the oracle pattern implicitly*[T5]. SCs are presented as *pseudo code*[T7] with *explicit performance testing*[T6]. They do not mention a *software engineering methodology*[T8] for developing this system.
[63]	In this article, Jensen et al. [63] discuss the *product*[T12] TradeLense that is introduced into the *logistics and shipment*[T11] domain. It uses *Hyperledger Fabric*[T10], *off-chain storage with relational databases*[T9] and supports *oracle patterns*[T5] as well as *proxy*[T4]-based architectures. The authors discuss a case study through several years and project steps, hence not going into detail in terms of SC *description*[T7] or *testing*[T6] or *software engineering methodology*[T8].

Continued on next page

ID	Description
[21]	Chaisawat et al. [21] present a *prototype*[T12] based on *Hyperledger Fabric*[T10] to extend the functionality of Immunization Information Systems to handle secure and authentic vaccination certificates in *healthcare*[T11], motivated by the Covid-19 outbreak. They employ *off-chain storage with IPFS*[T9] within a *proxy*[T4]-based architecture making *use of the oracle pattern implicitly*[T5]. They provide *pseudo code and diagrams*[T7] discussing the developed SCs and *explicitly conducted performance testing*[T6] but do not mention any *software engineering methodology*[T8].
[177]	To overcome existing limitations such as loss or fraud in the realm of *electricity retail contracts*[T11], the authors present a *Hyperledger Fabric*[T10]-based *prototype*[T12] that utilizes the blockchain properties of being immutable and tamper-resistant. By introducing a business layer between the application and blockchain layer, the architecture is classified as a *proxy*[T4]-based. The authors do not report on any used *software engineering methodology* [T8] but provide a *functional description*[T7] for the developed SCs with *implicit use of performance testing*[T6] *and usage of the oracle pattern*[T5]. Contract data is stored *off-chain in IPFS*[T9].
[36]	The study presented by Do et al. [36] introduces B4E, an *Ethereum*[T10]-based *prototype*[T12] aiming to ease the creation of digital *academic certificates*[T11]. They developed a *proxy*[T4] with an *implicit use of the oracle pattern*[T5]. The SCs are presented via *functional description*[T7] along with *implicit performance testing*[T6]. Document data is stored *off-chain in relational databases*[T9]. No *software engineering methodology*[T8] is mentioned in the paper.
[144]	Aiming to merge the ISO 19152 Land Administration Domain Model with evolving blockchain technology, Tahar et al. [144] present a *Hyperledger Fabric*[T10]-based *prototype*[T12] for *land administration*[T11]. They leverage *off-chain storage in a relational database*[T9] with the *implicit use of the oracle pattern*[T5] in a *proxy*[T4]-based architecture. The developed SCs are presented via *functional description*[T7] without mentioning SC *testing*[T6] or *software engineering methodologies*[T8].
[116]	This paper describes a *prototype*[T12] aiming for a more secure, traceable, and tamper-proof way of creating, sharing, and verifying *general digital credentials*[T11] such as academic certificates or personal identification documents. To achieve this goal, the authors use the *Hyperledger Fabric*[T10] blockchain in a *proxy*[T4]-based architecture with *off-chain storage in relational databases*[T9] and *implicit usage of the inbound-push*[T5] oracle pattern. The developed SCs are presented via *functional description*[T7] without discussing SC *testing patterns*[T6] or *software engineering methodologies*[T8].

Continued on next page

ID	Description
[117]	The study presents a *proposal*[T12] to use *blockchain*[T10] for creating digital *academic certificates*[T11] to overcome existing challenges such as lack of trust and centralized approaches. They describe an *on-chain*[T9] storage and a *proxy*[T4]-based architecture alongside an *implicit inbound-push*[T5] oracle pattern. In terms of proposed SCs, the authors provide *functional descriptions*[T7] but do not mention SC *testing*[T6] patterns or *software engineering methodologies*[T8] that they used to develop the proposed system.
[73]	Kumar et al. [73] present a *proposal*[T12] for a *blockchain-based*[T10] system to ease the verification process of candidates by providing tamper-resistant *academic certificates*[T11]. In their proposal, the authors argue to use *off-chain cloud storage*[T9] and present a *functional description*[T7] of potential SCs while neither discussing potential *testing patterns*[T6] nor *software engineering methodologies* [T8] that could aid the development of the proposed system. Derived from their functional description of SCs, they *implicitly use the oracle pattern*[T5] in a *proxy*[T4]-based architecture.
[130]	To overcome existing struggles such as data quality or authenticity in the context of calibration certificates (in this review categorized as *miscellaneous*[T11]), the authors present a *prototype*[T12] leveraging *IOTA*[T10]. Given the current limitations of executing SCs on IOTA, the authors are *not able to provide in-depth descriptions*[T7]. The same holds true for potential SC *testing*[T6] patterns. From the given diagrams and descriptions, it is derived that the authors developed a *proxy*[T4]-based system while using *the oracle pattern implicitly* [T5]. There is no insight given into a potentially used *software engineering methodology*[T8].
[32]	In order to enable tamper-resistant storage of *general digital documents*[T11], Deepika et al. [32] present an *Ethereum*[T10]-based *prototype*[T12]. Despite this goal, the paper does not provide SC *descriptions*[T7] nor potentially used *testing patterns*[T6] or a *software engineering methodology*[T8]. Based on the given description, the system leverages a *proxy*[T4]-based architecture and *implicitly uses the oracle pattern*[T5] along with *on-chain storage*[T9].
[49]	This paper presents a *proposal*[T12] to leverage *Hyperledger Fabric*[T10] to enable tamper-resistant digital *academic certificates*[T11]. They discuss a *proxy*[T4]-based architecture, *implicitly describing the oracle pattern*[T5]. Being only at an early proposal stage, the study does not include details in terms of SC *descriptions*[T7], *testing patterns*[T6], *storage*[T9] or a used *software engineering methodology*[T8].

Continued on next page

ID	Description
[60]	The study presented by Ionescu [60] shows the potential of blockchain-based e-prescription in the *healthcare*[T11] domain by discussing their *Ethereum*[T10]-based *prototype*[T12]. They make use of *off-chain*[T9] storage alongside an *implicit use of the oracle pattern*[T5]. The developed SCs are presented as *code*[T7] but without going into detail in terms of potential SC *testing*[T6] or *software engineering methodologies*[T8]. Derived from the presented system and implementation, it is classified as a *proxy*[T4]-based architecture.
[79]	The authors describe in this paper a novel blockchain-based approach to overcome the existing lack of transparency, openness, and potential fraud in terms of electronic seals (classified in this review under *miscellaneous*[T11]). They present a *blockchain agnostic*[T10], *proxy*[T4]-based *prototype*[T12] that leverages *off-chain storage with NoSQL databases*[T9], *implicitly using the oracle pattern*[T5]. Required SCs are presented via *functional description*[T7], not mentioning SC *testing*[T6] patterns or *software engineering methodologies*[T8].
[27]	Issues in the verification process of applicants' credentials are time-consuming, costly, and prone to forged or tampered credentials. The authors in this paper developed a *prototype*[T12] based on the *Hyperledger Fabric*[T10] blockchain enabling a tamper-resistant, fast and secure verification process of the applicants' *academic certificates*[T11]. The system leverages a *proxy*[T4]-based architecture with *off-chain storage in IPFS*[T9]. It *implicitly uses oracle patterns*[T5]. However, the paper lacks explanations in terms of developed *SCs*[T7], used *testing patterns*[T6], and *software engineering methodologies*[T8].
[65]	In this study, the authors discuss their developed *prototype*[T12] for a secure, tamper-resistant and transparent system for managing digital *academic certificates*[T11]. They make use of the *Hyperledger Fabric*[T10] blockchain and *off-chain storage with IPFS*[T9]. The system is integrated into a *proxy*[T4]-based architecture. While the paper does not provide insights into *SC descriptions*[T7], *testing patterns* [T6] nor *software engineering methodologies*[T8], it is derived from the general description that the system makes *implicitly use of the oracle pattern*[T5].
[69]	This paper highlights the potential benefits of employing blockchain technology in the process of *construction document*[T11] management. Even though the authors present a *prototype*[T12] of a *proxy*[T4]-based system, they *do not mention the underlying blockchain technology*[T10]. Likewise, there is *no detailed description for SCs*[T7], *testing patterns*[T6] or aused *software engineering methodology*[T8]. However, the authors describe the usage of *off-chain storage*[T9] and *the use of oracle pattern implicitly*[T5].

Continued on next page

ID	Description
[93]	Mutharasan et al. [93] present an *Ethereum*[T10]-based *prototype*[T12] to enable tamper-resistant digital *academic certificates*[T11] leveraging a *proxy*[T4]-based architecture. While they do *no go into greater detail in terms of SC descriptions*[T7], they do provide *explicit SC testing*[T6] insights. Furthermore, they leverage *off-chain storage with relational databases*[T9], *implicitly using oracle patterns*[T5]. The paper does not contain insights into a used *software engineering methodology*[T8].
[76]	The presented *prototype*[T12] in [76] highlights the potential of using blockchain (in this context *Hyperledger Fabric*[T10]) to create and manage digital invoices in the *construction*[T11] industry. They emphasize the privacy aspect in networks of potential competitors. The developed prototype follows a *proxy*[T4]-based architecture and leverages *off-chain*[T9] storage, thus *implicitly uses the oracle pattern*[T5]. While the general methodology of the paper follows the design science approach, no *software engineering methodology* [T8] is mentioned as well as *no detailed SC description*[T7] or SC *testing pattern*[T6].
[51]	This study discusses a *prototype*[T12] of a decentralized document management system for *general applicability*[T11]. It is based on the *Ethereum*[T10] blockchain in a *proxy*[T4]-based architecture using *off-chain storage in relational databases*[T9]. The authors provide insights into the developed SCs by providing *functional descriptions*[T7] from which an *implicit use of performance testing*[T6] is derived along with an *implicit use of the inbound-push oracle pattern*[T5]. No detail is given in terms of a used *software engineering methodology*[T8].
[173]	In this paper, the authors present an *Ethereum*[T10]-based *prototype*[T12] that leverages ciphertext-policy attribute-based encryption to ensure confidentiality and privacy in the context of cross-enterprise document sharing in the *healthcare*[T11] domain. The developed system uses *off-chain storage with IPFS*[T9] and, derived from the *functional description*[T7] of the developed SCs, *implicitly uses the inbound-push*[T5] oracle pattern. Furthermore, *implicit performance testing*[T6] for the SCs is derived based on the given description. The overarching architecture is classified as *proxy*[T4]-based. No insights into a used *software engineering methodology*[T8] is given.
[29]	The paper by Damian et al. [29] presents a *prototype*[T12] aimed at *general applicability*[T11] for digital document management based on blockchain. The authors leverage the *PrivateSKY*[T10] blockchain with *off-chain storage in relational databases*[T9] and an *implicit use of the oracle pattern*[T5]. The authors describe their transition from general software design patterns, i.e., moving from a model-view-controller approach to an action domain responder pattern, but they do not mention an overarching *software engineering methodology*[T8]. Required SCs are presented via *functional descriptions*[T7] without mentioning *testing patterns*[T6]. The overall architecture is classified as *proxy*[T4]-based.

Continued on next page

ID	Description
[140]	The *prototype*[T12] presented in Stana et al. [140] showcases a *Ethereum*[T10]-based system for managing *academic certificates*[T11]. It is classified as a *proxy*[T4]-based architecture and leverages *off-chain storage in relational databases*[T9] with an *implicit use of the oracle pattern*[T5]. The paper lacks of SCs *functional descriptions*[T7], *testing patterns*[T6] and a *software engineering methodology*[T8].
[64]	To ensure tamper-resistance of *academic certificates*[T11], Jovović et al. [64] present an *Ethereum*[T10]-based *prototype*[T12], aiming to put students in control of their academic identity. The system encompasses a dedicated back-end component between users and the blockchain layer, making it a *proxy-based*[T4] architecture. Documents and data are stored *off-chain in a relational database*[T9], *implicitly making use of oracle the pattern*[T5]. The authors do *not describe the SCs in detail*[T7], nor provide information on SC *testing*[T6] or a used *software engineering methodology*[T8].
[53]	Hasan et al. [53] highlight the potential of blockchain-based land documents overcoming current shortcomings of fraud, manual processes or ownership disputes in terms of *land administration*[T11]. They developed a *prototype*[T12] using *Ethereum*[T10] and *IPFS for off-chain storage*[T9]. Developed SCs are presented via *functional descriptions*[T7] without mentions of SC *testing patterns*[T6]. Derived from the descriptions, the system is categorized as *proxy*[T4]-based with an *implicit use of the oracle pattern*[T5]. No information about a used *software engineering methodology*[T8] is given.
[85]	The paper aims to enable users to verify *any kind of general digital document*[T11] only once and to save the result on a blockchain for future process optimization. The state of research focuses only on a *proposal*[T12], and *no specific blockchain*[T10] is chosen yet. Therefore, *SC descriptions* [T7] and *testing patterns*[T6] are not described. Based on the design proposal, their architecture is classified as *proxy*[T4]-based and *on-chain storage*[T9] of the checked results is considered favorable. The authors *implicitly designed an oracle pattern*[T5]. No *software engineering methodology* [T8] is mentioned.
[145]	This paper presents a *prototype*[T12] in the *healthcare*[T11] domain that leverages *Hyperledger Fabric*[T10] along with *IPFS as off-chain storage*[T9] to overcome the limitations of on-chain storage of large documents, which are used as input for artificial intelligence models. The authors developed a *dApp*[T4]-based architecture and *implicitly used the inbound-push*[T5] oracle pattern. However, *the paper lacks detailed SC descriptions*[T7] and *testing patterns*[T6] as well as an underlying *software engineering methodology*[T8].

Continued on next page

ID	Description
[96]	Investigating blockchain's potential as an enabler for fast, secure, and tramper-resistant digital *academic certificates*[T11] is the goal of Nguyen et al. [96]. The authors developed a *prototype*[T12] based on the *Ethereum*[T10] blockchain. They designed a *dApp*[T4]-based architecture in which the digital certificates are stored *off-chain in digital wallets*[T9]. The required SCs are presented making use of *diagrams*[T7] from which an *implicit inbound-push*[T5] oracle pattern is derived. The authors do not mention any SC *testing patterns*[T6], nor a *software engineering methodology*[T8].
[109]	Overcoming existing limitations of reliability and performance in the *land registration*[T11] system of Thailand, Pongnumkul et al. [109] developed a *prototype*[T12] using a private *Ethereum*[T10] blockchain. They developed a *dApp*[T4]-based system that uses *on-chain*[T9] storage. The necessary SCs are presented using *pseudo code*[T7]. From their description it is derived that an *inbound-push oracle pattern is implicitly used*[T5] alongside *implicit SC performance testing*[T6]. The authors do not mention any used *software engineering methodologies*[T8].
[152]	This paper presents a *prototype*[T12] of a decentralized document management system for *general applicability*[T11] using *Ethereum*[T10] blockchain alongside *IPFS for off-chain storage*[T9]. The authors provide a *functional description*[T7] for the developed SCs without mentioning *testing*[T6] patterns. Derived from the given description and overviews, the system is *dApp*[T4]-based and *implicitly uses the inbound-push oracle pattern*[T5]. It appears that no *software engineering methodology*[T8] is used in the development process.
[143]	In this study, the authors discuss their *Ethereum*[T10]-based *prototype*[T12] to create trustworthy and easy-to-verify digital *academic certificates*[T11]. They developed a *dApp*[T4]-based system where credentials are stored *off-chain in digital wallets*[T9]. The authors used a *functional description*[T7] of the SCs and *explicitly performed and mentioned SC testing*[T6] while also *explicitly mention the usage of the inbound-push oracle pattern*[T5]. However, they do not mention an overarching *software engineering methodology*[T8].
[40]	To tackle the issue of fraud related to forged academic certificates in Egypt, El-Dorry et al. [40] present a *prototype*[T12] based on *Hyperledger Fabric*[T10] to create tamper-resistant and trustworthy digital *academic certificates*[T11] stored *on-chain*[T9]. They developed a *dApp*[T4]-based architecture, *implicitly using the oracle pattern*[T5]. However, the paper does not report SC *functional descriptions*[T7], *testing patterns*[T6] or the used *software engineering methodology*[T8].

Continued on next page

ID	Description
[100]	Notland et al. [100] present an *Ethereum*[T10]-based *pilot*[T12] that aims to tackle fraud and corruption by developing minimum hybrid contracts that combine smart contract and legal contracts (sorted into the *miscellaneous*[T11] category). They do not detail their *document storage*[T9] but provide *functional descriptions*[T7] of the developed SCs from which an *implicit usage of the oracle pattern*[T5] is derived. *Testing patterns*[T6] or a *software engineering methodology*[T8] are not mentioned. In general, the architecture is categorized as *dApp*[T4].
[1]	This paper highlights an *Ethereum*[T10]-based *dApp*[T4] architecture that *prototypes*[T12] the management of digital *academic certificates*[T11]. The authors provide *functional descriptions*[T7] of the developed SCs along with *on-chain*[T9] storage and *explicit mention of the inbound-push oracle pattern*[T5]. The used *testing patterns*[T6] or a underlying *software engineering methodology*[T8] cannot be derived.
[55]	In this study, the authors focus on a multi-signature process for signing and creating *academic certificates*[T11] based on the *Ethereum*[T10] blockchain. Their *prototype*[T12] is *dApp*[T4]-based and *implicitly implements the inbound-push oracle pattern*[T5]. The authors provide a *functional description*[T7] for the developed SCs but *no testing patterns*[T6] or *software engineering methodology*[T8]. Documents and data are stored *on-chain*[T9].
[52]	To overcome shortcomings of digital documents such as the lack of authenticity, integrity, and being prone to forgery, Harlian et al. [52] present a *prototype*[T12] based on *Ethereum*[T10] and *on-chain*[T9] storage for *general applicability*[T11]. Their system is based on a *dApp*[T4]-architecture and *implicit oracle patterns*[T5]. The authors provide *diagrams*[T7] for the description of developed SCs as well as *explicit performance tests*[T6]. There is no indication of an explicitly used *software engineering methodology*[T8].
[6]	This study presents an *Ethereum*[T10]-based *prototype*[T12] that aims to leverage blockchain properties to overcome existing limitations in authenticity and reliance on third parties for current digital document management. The authors describe a system for *general applicability*[T11] using a *dApp*[T4]-based architecture, mitigating the need for (trusted) third parties. Developed SCs are presented as *functional descriptions*[T7] along with an *implicit use of performance testing*[T6]. The authors use *IPFS as off-chain storage*[T9]. Derived from the presented system, it *implicitly uses the oracle pattern*[T5]. No underlying *software engineering methodology*[T8] for the development process is mentioned.

Continued on next page

ID	Description
[59]	Optimizing the current process of (digital) document verification to be transparent and traceable is the goal of Imam et al. [59]. They developed a *prototype*[T12] using a *dApp*[T4]-based architecture with an underlying *Ethereum*[T10] blockchain. They provide a *functional description*[T7] of the required SCs along with an *off-chain storage approach with IPFS*[T9]. The developed system aims to be *generally applicable*[T11] for all sorts of digital documents. Derived from the given descriptions, the authors followed *the oracle pattern implicitly*[T5]. They do not describe any used *software engineering methodology*[T8] or SC *testing*[T6].
[133]	To enhance security and performance in the *land administration*[T11] process, the authors present a *proposal*[T12] arguing for an *Ethereum*[T10]-based *dApp*[T4] leveraging *IPFS as off-chain storage*[T9], also *implicitly describing the usage of the oracle pattern*[T5]. They provide a *functional description*[T7] for the to-be implemented SCs but do not detail any *testing pattern* [T6] or a *software engineering methodology*[T8].
[120]	In this paper, the authors discuss the potential of developing an *Ethereum*[T10]-based *dApp*[T4] for creating and verifying digital *academic certificates*[T11] to overcome existing limitations such as authenticity and integrity of issued certificates. They further propose *on-chain*[T9] storage along with a *functional description*[T7] of the SCs validating certificates on-chain. Since the paper's scope is a *proposal*[T12], a presentation of SC *testing patterns*[T6] or a *software engineering methodology*[T8] is missing. Based on the presented descriptions, it is derived that the authors *implicitly use the oracle pattern*[T5].
[101]	The study presented by Oh et al. [101] describes a developed *dApp*[T4] *prototype*[T12] based on the *MultiChain*[T10] blockchain to digitize documents in e-trade (categorized in the *miscellaneous*[T11] category). The authors leverage *on-chain*[T9] storage and present *functional descriptions*[T7] for the developed SCs. From their description, it is derived that they *implicitly use the oracle pattern*[T5]. The paper does not provide details in terms of SC *testing*[T6] patterns or used *software engineering methodologies*[T8].
[164]	Wu et al. [164] present in their paper a *Hyperledger Fabric*[T10]-based *prototype*[T12] to enhance current journal submission processes by detecting multiple submission while ensuring the authenticity and immutability of the manuscripts (categorized into *miscellaneous*[T11]). The authors developed a *dApp*[T4] but without presenting details in terms of *SC descriptions*[T7], SC *testing patterns*[T6], the used *software engineering methodologies*[T8]. Derived from the description of the system, the authors *implicitly employ the oracle pattern*[T5] along with *off-chain storage in IPFS*[T9].

Continued on next page

ID	Description
[26]	To overcome fraud and centralization and achieve security and efficiency, the authors of this study present a *prototype*[T12] based on *Hyperledger Fabric*[T10] and *IPFS for off-chain storage*[T9] to create a system for managing *general*[T11] digital documents. They developed a *dApp*[T4] and derived from the given *functional description*[T7] of SCs, they *implicitly make use of the oracle pattern*[T5] but do not detail any SC *testing patterns*[T6] nor the used *software engineering methodology*[T8].
[163]	In this paper, a blockchain-based *prototype*[T12] for electronic stamp duty for tax documents (categorized as *miscellaneous*[T11]) is presented. *Ethereum*[T10] is used as the underlying blockchain to build a *dApp*[T4] with *on-chain storage*[T9]. The authors present a *functional description*[T7] for the developed SCs without mentioning SC *testing patterns*[T6] or *software engineering methodologies*[T8]. Derived from the given description, the system *implicitly uses the oracle pattern*[T5].
[20]	Ensuring authenticity and longevity of *academic certificates*[T11] is the goal of Budhiraja and Rani [20]. The authors present a *dApp*[T4] *prototype*[T12] based on *Ethereum*[T10] and *IPFS for off-chain storage*[T9]. They provide *functional descriptions*[T7] of SCs, not mentioning *testing patterns*[T6] or a *software engineering methodology*[T8]. Derived from the description of the system, the authors *implicitly used the oracle pattern*[T5].
[126]	In this study, the authors *propose*[T12] to use a blockchain-based approach (*not*[T10] focusing on a specific blockchain) to overcome digitization limitations of *personal documents*[T11] such as counterfeits or privacy risks. The authors use *off-chain storage via IPFS*[T9] in a *dApp*[T4]-based architecture. Given the proposal stage, the authors do not present *SC descriptions*[T7], *testing patterns*[T6], or a *software engineering methodology*[T8] that could be used when implementing such a system. Derived from the system description, the authors *implicitly suggest the oracle pattern*[T5].
[151]	The paper presented by Vairagkar and Patil [151] showcases a *proposal*[T12] to use blockchain technology to enable fast and secure verification of *academic certificates*[T11]. The authors *do not specify*[T10] which specific blockchain to use but argue for *on-chain storage*[T9]. They propose the development of a *dApp*[T4] and present *functional descriptions*[T7] for the SCs. There are no insights into SC *testing patterns*[T6] or *software engineering methodologies*[T8]. Based on the given description, the authors will *implicitly require an oracle pattern* [T5] even though they did not mentioned it.
[98]	Nizamuddin et al. [98] present a *dApp*[T4]-based *prototype*[T12] utilizing the *Ethereum*[T10] blockchain and *IPFS for off-chain storage*[T9] to enable secure and tamper-resistant document management for *general applicability*[T11] and multi-user collaboration. The developed SCs are presented via *functional description*[T7] along with *explicit mentions of security testing*[T6]. Given the description, it is derived that the system *implicitly uses the oracle pattern*[T5]. No *software engineering methodology*[T8] is named.

Continued on next page

ID	Description
[97]	This paper presents a *prototype*[T12] for the *healthcare*[T11] domain showcasing the potential of blockchain-technology in terms of access-control and secure, tamper-resistant storage of medical reports, documents and data. The authors design and implement a *dApp*[T4] based on the *Ethereum*[T10] blockchain. They make use of *on-chain storage*[T9] and *implicitly used the oracle pattern*[T5] which is derived from the provided *functional descriptions*[T7] of the SCs. The authors do not mention SC *testing*[T6] or a *software engineering methodology*[T8].
[131]	In this study, the authors present a *dApp*[T4] *prototype*[T12] based on *Ethereum*[T10] to digitize and manage digital *healthcare*[T11] documents in a secure and decentralized way. They opt for *on-chain storage*[T9] and *implicitly use the oracle pattern*[T5]. The developed SCs are presented via *functional descriptions*[T7] with *explicit performance testing*[T6]. There is no overarching *software engineering methodology*[T8] mentioned.
[77]	To enhance existing blockchain-based systems for digital *academic certificates*[T11] with an audit-ability feature, Le et al. [77] present a novel data structure called Auditable Merkel Tree which they combined with the *Ethereum*[T10] blockchain. They present the developed SCs as *code*[T7] and *explicitly highlight conducted security testing*[T6]. Derived from their paper, the developed *dApp*[T4] is in a *prototype*[T12] state and *the oracle pattern is implicitly used*[T5] alongside *off-chain storage*[T9]. The authors do not mention *software engineering methodologies*[T8].
[107]	In this paper an *Ethereum*[T10]-based *dApp*[T4] *prototype*[T12] is presented, aiming to enable and improve digital signing for *general*[T11] digital documents. The authors present the developed SCs on a *code*[T7]-level, from which the *implicit use of the oracle pattern*[T5] is derived. The paper does not contain details about *storage*[T9], SC *testing patterns*[T6], or *software engineering methodologies*[T8].
[33]	The presented *prototype*[T12] in [33] aims to improve the authenticity and transparency of *academic certificates*[T11] by developing an *Ethereum*[T10]-based *dApp*[T4] that leverages *off-chain storage with a NoSQL database*[T9]. The implemented SCs are presented via *functional descriptions*[T7], from which an *implicit use of performance testing*[T6] and *the oracle pattern*[T5] are derived. The paper does not mention a *software engineering methodology*[T8].
[11]	In order to ensure privacy and authenticity for document sharing in the *construction*[T11] domain, the authors present a *prototype*[T12] built on the *Ethereum*[T10] blockchain. Their developed system is *dApp*[T4]-based and relies on *IPFS as means for off-chain storage*[T9]. The required SCs are presented as part of the *functional description*[T7] of the system, not detailing any *testing patterns*[T6] or a *software engineering methodology*[T8]. Based on the given description, the system *implicitly uses the oracle pattern*[T5].

Continued on next page

ID	Description
[62]	This study aims to overcome limitations in existing systems such as scalability, privacy, and authenticity in the *healthcare*[T11] domain by leveraging the *Polygon Matic*[T10] blockchain technology. The authors developed a *dApp*[T4] *prototype*[T12] using *IPFS for off-chain storage*[T9]. While they did not mention a dedicated *software engineering methodology*[T8], they present the developed SCs using *diagrams*[T7] and conducted *explicit SC testing*[T6]. From the given description an *implicit use of the oracle pattern*[T5] is derived.
[75]	The paper by Lalitha et al. [75] presents a *Ethereum*[T10]-based *dApp*[T4] *prototype*[T12] for *general applicability*[T11] for digital documents. They leverage *on-chain storage*[T9] but do not go into detail about *SC descriptions*[T7], SC *testing patterns*[T6], or *software engineering methodology*[T8]. Derived from the description of the system, they *implicitly use the oracle pattern*[T5].
[61]	Islamay et al. [61] present a *dApp*[T4] *prototype*[T12] based on the *Ethereum*[T10] blockchain to create a system for *general*[T11] digital document management, enabling a transparent and tamper-resistant system. They provide a *functional description*[T7] for the developed SCs and make use of *IPFS for off-chain storage*[T9], *implicitly using the oracle pattern*[T5]. They do not provide insights into SC *testing patterns*[T6] or an employed *software engineering methodology*[T8].
[105]	An *Ethereum*[T10]-based *dApp*[T4] *prototype*[T12] is presented that enables the citizens' sovereignty over their *personal documents*[T11] while preserving privacy and data authenticity. The authors make use of *on-chain storage*[T9] to ensure tamper-resistance and present their developed SCs with *functional descriptions*[T7], along with *explicit security testing*[T6]. Derived from their description, they *implicitly use the oracle pattern*[T5] but do not mention any specific *software engineering methodology*[T8] that has been followed.
[2]	In this study, the authors leverage a *dApp*[T4] *prototype*[T12] based on the *Ethereum*[T10] blockchain to build a decentralized identity and access management system that enables transparent and secure management of *personal documents*[T11]. Based on their paper, the authors did not follow a specific *software engineering methodology*[T8] when developing the SCs that are presented as *code*[T7]. They do not go into detail in terms of SC *testing*[T6]. The system leverages *on-chain storage*[T9] and *implicitly uses the oracle pattern*[T5].

Continued on next page

ID	Description
[162]	The paper presented by Westphal et al. [162] discusses the potential of using the *Ethereum*[T10] blockchain in additive manufacturing to capture and share quality-related data and documents of the manufacturing process in a secure and tamper-resistant way (categorized into *miscellaneous*[T11]). The authors discuss their developed *prototype*[T12] and highlight SCs using *diagrams*[T7]. Their system is *dApp*[T4]-based and uses *off-chain storage via IPFS*[T9]. Given their description, it is derived that the system *implicitly implements the oracle pattern*[T5]. No information about SC *testing patterns*[T6] or a *software engineering methodology*[T8] is given.
[129]	Sarang et al. [129] showcases their *prototype*[T12] based on the *Polygon*[T10] blockchain that aims to ensure tamper-resistant, secure and private management of *personal documents*[T11]. They used *IPFS for additional off-chain storage*[T9] and present *code*[T7] of the developed SCs as part of their *dApp*[T4]. The paper does not provide insights into the used SC *testing patterns*[T6] or the followed *software engineering methodologies*[T8]. Drawing from the description, they *implicitly used the oracle pattern*[T5].
[114]	In this paper, the authors leverage *IPFS for off-chain storage*[T9] to overcome existing blockchain-related limitations in storage and scalability. Their *prototype*[T12] addresses the use case of *academic certificates*[T11]. They developed a *dApp*[T4] based on the *Ethereum*[T10] blockchain and conducted *implicit performance testing*[T6]. The SCs are presented as *functional description*[T7] from which the *implicit use of the oracle pattern*[T5] is derived. No insights in terms of *software engineering methodologies*[T8] are given.
[38]	To provide secure and forgery-proof means of digital *academic certificates*[T11], Dumpeti and Kavuri [38] designed and developed a *prototype*[T12] based on the *Hyperledger Fabric*[T10] blockchain. Their developed *dApp*[T4] relies on *on-chain*[T9] storage along with an *implicit usage of the oracle pattern*[T5]. The paper does not contain detailed insights into the *SCs*[T7], but an *implicit use of performance testing*[T6] can be derived. No particular *software engineering methodology*[T8] is mentioned.
[35]	This study highlights blockchain's properties of immutability and authenticity for *general digital documents*[T11] in the context of a digital notary service in Brazil. The authors investigate this potential by developing a *dApp*[T4] *prototype*[T12] based on the *Ethereum*[T10] blockchain. Data and documents are stored in the *IPFS as off-chain storage*[T9] where the authors mention the usage of the *inbound-push oracle pattern explicitly*[T5]. They provide a *functional description*[T7] for the developed SCs but do not detail *SC testing patterns*[T6] or a *software engineering methodology*[T8].

Continued on next page

ID	Description
[17]	The authors of this paper present a *Ethereum*[T10]-based *dApp*[T4] to manage warranty receipts (grouped into the *miscellaneous*[T11] category) in a fraud-resistant way. Based on their *functional description*[T7] of the SCs and *prototype*[T12], they *implicitly use the oracle pattern*[T5] and employ *IPFS for off-chain storage*[T9]. The authors do not mention specific SC *testing patterns*[T6] or *software engineering methodologies*[T8].
[56]	To overcome the existing limitation of the weak connection between *academic certificates*[T11] and the recipients in blockchain-based systems, the authors propose the combination of biometrics and cryptography in a *Hyperledger Fabric*[T10]-based *prototype*[T12]. They conducted *implicit performance testing*[T6] of their developed *dApp*[T4] but *do not provide detailed description*[T7] of the developed SCs nor the used *software engineering methodologies*[T8]. Derived from the system description, the authors *implicitly used the oracle pattern*[T5] along with *on-chain storage*[T9].
[171]	Yousef [171] developed a *prototype*[T12] based on an *Ethereum*[T10] blockchain to enable tracking students' progress and to issue and verify *academic certificates*[T11]. Their *dApp*[T4] makes use of *on-chain*[T9] storage with *implicit use of the oracle pattern*[T5] and they present *code*[T7] for the developed SCs. The authors do not offer insight into SCs *testing patterns*[T6] or a used *software engineering methodology*[T8].
[112]	In this study, the authors *propose*[T12] to use blockchain as a secure system to transfer ownership and manage *land registrations*[T11]. The authors do not suggest any *architecture*[T4], *blockchain*[T10] , *storage*[T9], SC *testing*[T6] or *software engineering methodology*[T8]. However, they provide a *functional description*[T7] for the to-be developed SCs, from which an *implicit use of the oracle pattern*[T5] is derived.
[7]	In this paper, Alvi and Iqbal [7] present a *prototype*[T12] for managing and verifying digital *academic certificates*[T11] making use of the *Ethereum*[T10] blockchain. Despite presenting a prototype, the paper does not provide insights into the *architecture*[T4], SC *descriptions*[T7], SC *testing patterns*[T6], *software engineering methodology*[T8], or *storage*[T9]. Derived from the system description, it leverages the *oracle pattern implicitly*[T5].
[135]	The developed *prototype*[T12] in this paper aims to enable secure and tamper-resistant issuance and verification of *academic certificates*[T11] leveraging the *Ethereum*[T10] blockchain. Next to a *functional description*[T7] of developed SCs, the authors also explain the usage of *off-chain storage using IPFS*[T9]. From this it is derived that the system *implicitly uses the oracle pattern*[T5]. No answer is given for the used *architecture*[T4] the context of used SC *testing patterns*[T6], or *software engineering methodology*[T8].

Continued on next page

ID	Description
[118]	This study presents a *proposal*[T12] highlighting the benefits of a fast and secure verification of *academic certificates*[T11]. Given the early stage of the proposal, the authors focus on the general functionality of the system, not detailing the *architecture*[T4], *used blockchain*[T10], *storage*[T9], *SC description* [T7], SC *testing*[T6] or *software engineering methodology*[T8]. However, from the description, the need for the *oracle pattern is implicitly* [T5] derived.
[4]	The paper presented by Aldwairi et al. [4] showcases a *Ethereum*[T10]-based *prototype*[T12] to enable secure and fast verification of *academic certificates*[T11]. Derived from the system description, it *implicitly uses the oracle pattern*[T5]. Next to a *functional description*[T7] for the required SCs, the authors do not detail any SC *testing patterns*[T6], *storage*[T9], *architecture*[T4] or *software engineering methodology*[T8].
[83]	In this study, the authors present an *Ethereum*[T10]-based *prototype*[T12] in the domain of *academic certificates*[T11]. Data and documents are stored in *IPFS as off-chain*[T9] storage, *implicitly using the oracle pattern*[T5]. The authors further provide a *functional description*[T7] along with *implicit performance testing*[T6] but without going into details about *architecture*[T4] or *software engineering methodology*[T8].
[8]	Antoni et al. [8] *propose*[T12] a design for a blockchain-based system for managing *personal documents*[T11] in e-government services. They leveraged *rapid application development*[T8] for their design and argue for *off-chain storage using NoSQL databases*[T9], indicating *implicit usage of the oracle pattern*[T5]. The paper does not present further insights into the underlying *blockchain*[T10], *architecture*[T4], SC *description*[T7] or *testing patterns*[T6].
[9]	This paper presents a *proposal*[T12] to use blockchain technology as a means for secure management and verification of *academic certificates*[T11]. The authors argue for the use of *on-chain*[T9] storage from which an *implicit oracle pattern*[T5] is derived. However, the paper does not provide information in terms of underlying *blockchain*[T10], *architecture*[T4], SC *description*[T7], *testing patterns*[T6] or *software engineering methodology*[T8].
[68]	The study presented by Khanna et al. [68] uses *Ethereum*[T10] for securing digital *academic certificates*[T11]. In the design of their *prototype*[T12], they argue for *cloud storage as means for off-chain storage*[T9] from which an *implicit use of the oracle pattern*[T5] is derived. The authors do not go into detail about *architecture*[T4], SC *description*[T7], *testing patterns*[T6] or *software engineering methodology*[T8].

Continued on next page

ID	Description
[153]	In their presented *prototype*[T12], the authors discuss an *Ethereum*[T10]-based system for *general*[T11] digital documents. To ensure the privacy of managed documents, the authors employ *IPFS for off-chain storage*[T9] leading to an *implicit use of the oracle pattern*[T5]. Next to a general *functional description*[T7] of SCs, the paper does not provide further details about *architecture*[T4], *software engineering methodology*[T8] or SC *testing patterns*[T6].
[169]	In order to decrease the authentication time and enhance the authenticity of *land registration*[T11] data and documents, Yadav et al. [169] present a *prototype*[T12] leveraging blockchain technology. The proposed system is *blockchain agnostic*[T10] but relies on *IPFS for off-chain storage*[T9]. The authors use *the oracle pattern implicitly*[T5] and their description *implies performance testing*[T6]. They do not provide details about SC *description*[T7], *architecture*[T4] or *software engineering methodologies*[T8].
[119]	This study presents an *Ethereum*[T10]-based *prototype*[T12] aiming to optimize the verification process of digital *academic certificates*[T11]. While the description of the *architecture*[T4] remains opaque, the proposed usage of *IPFS for off-chain storage*[T9] is clear. Derived from this, the system *implicitly uses the oracle pattern*[T5]. No information could be derived regarding used *software engineering methodologies*[T8], SC *descriptions*[T7] or *testing patterns*[T6].
[172]	To further enhance and protect *general*[T11] electronic documents, Yuan et al. [172] *propose*[T12] the combination of ciphertext-policies attributed based encryption in combination with blockchain. Their proposed approach is *blockchain agnostic*[T10] and leverages *on-chain*[T9] storage leading to an *implicit usage of the oracle pattern*[T5]. Given the early stage of this proposal, the paper does not detail any SC *descriptions*[T7], *testing patterns*[T6], *software engineering methodologies*[T8] or *architecture*[T4].
[37]	Dumpeti and Kavuri [37] *propose*[T12] a *Hyperledger Fabric*[T10]-based system for *academic certificates*[T11] to tackle forging attempts. From their description, it is derived that the system *implicitly deploys the oracle pattern*[T5]. However, the authors do not provide details in terms of *storage*[T9], *architecture*[T4], *software engineering methodologies*[T8] or SC *descriptions*[T7] and *testing*[T6].
[82]	A *pilot*[T12] study for digital *academic certificates*[T11] in Moroccan Universities is presented in this study. The authors describe an *IPFS-based off-chain storage*[T9] but do not mention the underlying *blockchain*[T10] technology or *architecture*[T4]. They present *functional descriptions*[T7] for the used SCs from which an *implicit use of the oracle pattern*[T5] is derived. There are no further details in terms of SC *testing*[T6] or used *software engineering methodologies*[T8].

Continued on next page

ID	Description
[103]	In their *proposal*[T12], Pal and Kumar [103] argue to leverage blockchain technology (not mentioning a specific *blockchain*[T10]) alongside QR codes to enable for quick and secure verification of *general*[T11] documents. In their proposal, the authors describe *on-chain storage*[T9] from which an *implicit use of the oracle pattern*[T5] is derived. The paper does not provide details in terms of SC *description*[T7], *architecture*[T4], *testing*[T6] or used *software engineering methodologies*[T8].

Received 29 June 2024; revised 24 January 2025; accepted 6 May 2025