Blockchain-based Access and Usage Control of Government Systems, Educational Systems, and Electronic Health Records.

Austin Tokar, Emma Cunningham, and Jason Bailey

Pennsylvania State University, Monaca, United States

Abstract-- Blockchain technology has been based as a secure and transparent solution for the management of sensitive data. However, access and usage control in government, education, and electronic health record (EHR) systems still face significant problems. These problems include data breaches, lack of good accountability, and low trust among involved parties. One of the main goals of the blockchain framework is to offer a decentralized and unbreakable control, but their incorporation into the existing systems brings complicated technical and organizational issues. The proposed framework in the paper shows the use of smart contracts in policy enforcement with a focus on critical areas. It increases the level of transparency and trust among the parties, while decreasing the role of the central authorities, that is the case in traditional setups. The results of our study demonstrate very promising possibilities for getting rid of unauthorized access while at the same time assuring compliance and trust in digital communication. The results cast blockchain as a building block for the coming generations of access and usage control.

Keywords—Blockchain, Smart Contracts, Electronic health records (HER),…

1 Introduction

In the digital world that is fast becoming the norm, the management of data in a manner that is both secure and transparent has turned to be a primary issue in the case of government, education, and healthcare. Protection against unauthorized access is a must for sensitive data like citizen records, academic credentials, and electronic health records (EHRs) whereas the authorized ones should find the information readily available. Centralized traditional access control mechanisms are most often linked with the drawbacks of data breaches, single points of failure, and lack of accountability. However, blockchain technology advancement appears as a promising alternative. By creating a decentralized, tamper-free and transparent ledger, blockchain accesses and usage controls the traditional systems can't provide anymore.

Compared with current methods, the solutions based on Blockchain are the main reason behind the leading-edge authorization, non-alterable audit trails, and interactions among the parties without having to trust one another. In the case of government systems, this effect will not only help in getting better public trust but also making sure that the records are safe, easy to verify, and immune to any kind of changing. The question of who can access which part of a digital twin, and under what conditions, stops being a technical detail and becomes a core governance issue. In case of academic systems, it would be easy to verify students' degrees, get rid of cheating and facilitate sharing of data among the institutions, thanks to blockchain. Not only does it secure sensitive patient data in a hospital, but it also makes it easy and safe for providers with permission to access the records, all at once cutting the healthcare sector in half of its blockchain patient data issue. All these together show the potential of blockchain as a game-changing application for the protection of vital information infrastructures.

2 Electronic Health Records

An electronic health record (EHR) is a digital version of a patient's health record, containing sensitive information about their history, diagnosis, and treatment. EHR data usually covers appointments, billing, and lab tests. Early leaders in EHRs include Indiana University, the Mayo Clinic, and Vanderbilt University. In the 70s, the federal government created VistA, the largest EHR system, for Veterans Affairs. EHRs become more popular in 1992 as computer technology improved, and hardware costs dropped in price. The Health Information Technology for Economic and Clinical Health Act (HITECH) in 2004 showed the need to switch to EHRs, with incentives and resources available from the American Recovery and Reinvestment Act (ARRA or "Obamacare") starting in 2009. In 2017, around 95% of American hospitals were using EHR systems.

The integration of blockchain technology into electronic health records systems presents a game-changing approach to improve access and usage control. This can help address critical challenges related to data security, privacy, and interoperability. (Blockchain is a secure way to share information across a computer network).

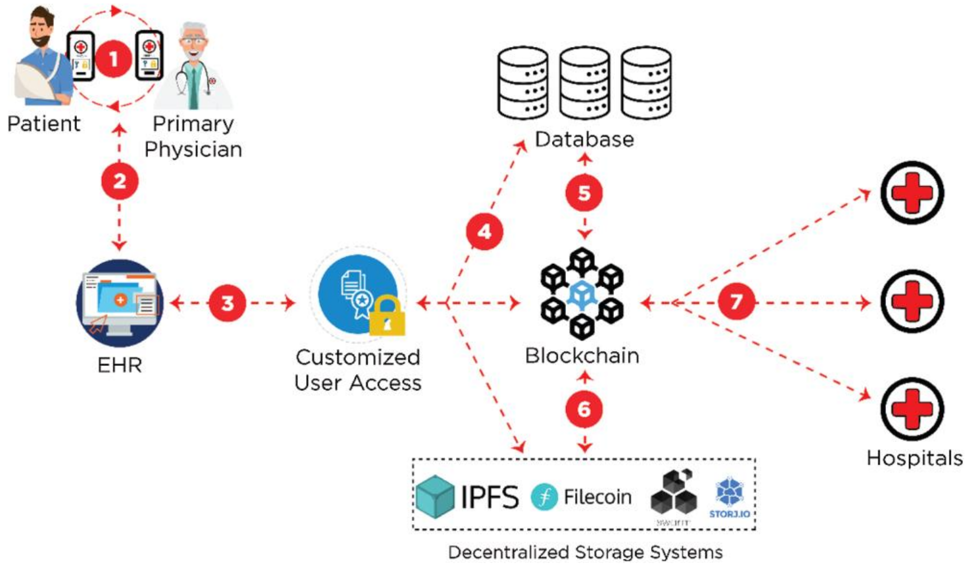


Fig. 1 : Blockchain-enabled EHRs management in healthcare by techscience

Traditional EHR systems often suffer from centralized data storage, making them vulnerable to breaches and unauthorized access. Blockchain can have a decentralized and immutable nature. This can offer a robust framework for securing patient data by employing cryptographic techniques and distributed consensus mechanisms. Blockchain can help ensure that every transaction and access attempt is recorded and verified across a network of nodes. This can help enhance transparency and accountability. This innovative application has the potential to transform healthcare data management. By providing patients with greater control over their health information. They can do this while streamlining administrative processes for healthcare providers.

The Healthcare based Blockchain is used for monitoring remotely and accessing business health records. Also, some hospitals use a private blockchain based on Ethereum to keep patient data private and safe. This helps keep a secure log of who’s done what on the blockchain. This can be very detailed for every data transaction. After that the system will send out notifications that go out to everyone involved.

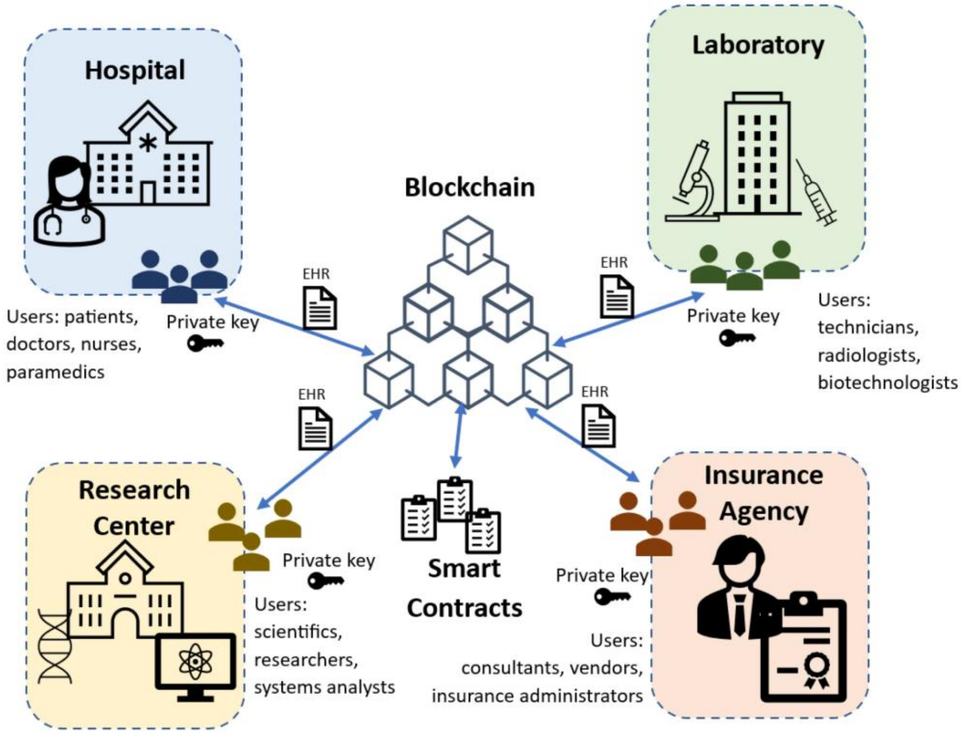
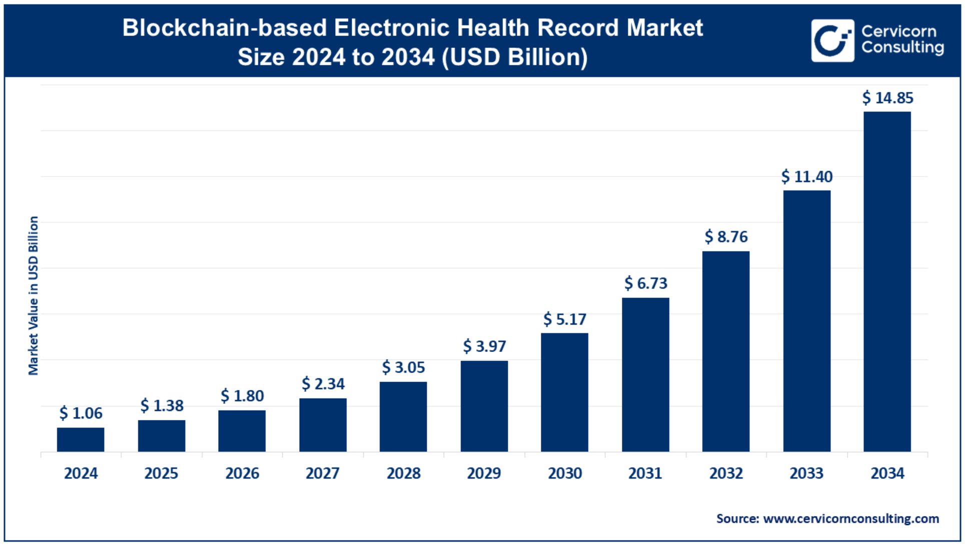

Hospital
Laboratory
Blockchain
EHR
EHR
EHR
EHR
Users: patients, doctors, nurses, paramedics
Private key
Private key
Users: technicians, radiologists, biotechnologists
Research Center
Private key
Users: scientifics, researchers, systems analysts
Smart Contracts
Insurance Agency
Private key
Users: consultants, vendors, insurance administrators

Fig. 2 : Scheme of the proposed architecture using four organizations: Hospital, Laboratory, Research Center, and Insurance Agency. By mdpi

This can help fix security issues in remote patient monitoring and other a lot of other issues. Many hospitals can use frameworks to help secure and make the systems better like MPC (Secure Multiparty Computing), Indicator-Centric Schema (ICS), and Healthcare Data Gateway (HGD. Digital twins in healthcare require continuous data exchange between physical and digital components, and the security that protects these exchanges is essential because any compromised data can lead to a compromised twin. This can be used as long as it is with blockchain. The hospitals need to make sure patients can easily and safely own, control, and share their data. MeDShare uses smart contracts and access contracts and access control to monitor how patient privacy data is used and spot any privacy breaches. They closely track all actions on the data smart contracts and keys. The system does this, so no one attempts to steal data or mess with reports that can be or are exposed. This can lead to restricted or revoked access. Many studies use blockchain to store, track, and manage medical records. Researchers are suggesting an IoMT (Internet of Medical Things) and blockchain to encrypt and save health information. Smart sensors collect health data, which is then encrypted and stored on the Ethereum blockchain, protecting user privacy.

Current trends for EHR are very helpful for research and development in blockchain-based access and usage control of electronic health records (EHRs). There is a lot to heavily focus on several key areas. This includes creating interoperability solutions to ensure that blockchain-based EHR systems can work seamlessly with existing healthcare IT infrastructure. Efforts are also being directed toward scalability improvements, aimed at enhancing the ability of blockchain networks to handle the large volume of healthcare data. Many researchers are exploring and finding easier ways to enhance security measures. One of the major ways is new cryptographic techniques and consensus mechanisms to further strengthen and the security of blockchain-based EHR systems. Smart contract innovations are also a significant focus. This can help developers create more sophisticated smart contracts to automate and enforce fine-grained access control policies. Finally, research is concentrating on integrating privacy preserving technologies, like zero-knowledge proofs and homomorphic encryption, to protect sensitive patient data on blockchain.


Blockchain-based Electronic Health Record Market Size 2024 to 2034 (USD Billion)

Source: www.cervicornconsulting.com

Fig. 3: Future prediction by Cervicorn Consulting

Current and future trends are very important to the future of HRE, focusing on improving data security, patient empowerment, and interoperability. The reason for this is that it is very important to focus on improving it to help keep people safe and prepare for anything like accidents or mistakes. There is a big push in the health field towards using more sophisticated smart contracts to automate and enforce access policies. The hospitals want to ensure that only authorized parties can access specific data. There are more systems that are being designed to give patients greater control over their data. Blockchain makes all this easier. It is very important for the hospital to grant or revoke access as they see fit for the policy. Finally, there’s a growing emphasis on making these blockchain solutions work seamlessly with existing healthcare systems to improve data sharing and coordination of care. Current and Future research is focusing on exploring more ways to make blockchain-based health records more scalable and user-friendly. This can benefit the elderly community a lot. The health field could focus on better encryption, faster transaction speeds, and easier ways for patients and doctors to use the system.

There are a lot of key advantages to blockchain-based access control. It can focus on the ability to enforce fine-grained permissions and usage policies.

The hospitals can use Smart contracts and self-executing agreements written in the blockchain. This can help regulate data access based on predefined rules. For example, this can help patients grant temporary access to a specific doctor or researcher. So, with the smart contract automatically can revoke access upon expiration. Furthermore, blockchain facilitates can help to secure data sharing between different healthcare providers and institutions. This can help improve care coordination and ensure that only authorized parties can access specific portions of a patient's record, maintain confidentiality and comply with stringent regulatory requirements such as HIPAA

Blockchain technology in healthcare has some disadvantages, including scalability issues that can slow down network efficiency when processing large volumes of users. The complexity of implementing and managing blockchain systems requires specialized expertise. This can pose a challenge for widespread adoption. Regulatory uncertainty due to the absence of clear legal frameworks further hinders its progress. Additionally, the high costs associated with establishing and maintaining a blockchain infrastructure can be a significant barrier for many organizations.

The current and future trends for healthcare-based blockchain based on the research are here to stay and it truly good. It has helped make it is way easier for both employees and patients. There is a lot of useful information that the blockchain keeps safe and managing for both employees and patients. It is very important to have a safe and fast way to provide sensitive information to each other in the network of healthcare. Blockchain is a lot faster and easier to use than what hospitals were doing before. With blockchain, there are a lot of possibilities in the future. I truly believe the advances outweigh the disadvantages of blockchain in the health field.

3 Educational Systems

The rapid growth of digital learning technologies has completely changed how educational institutions manage student records. As more learning takes place online like online classes which I am currently taking. Students will begin to accumulate credentials across different institutions and different platforms. Unfortunately, traditional data systems, to say the least, have struggled to keep pace with modern needs. Keeping track of credits, diplomas, and credentials has become more and more difficult over time. Centralized database systems have slow verification procedures. Their fragmented credentialing practices limit students' abilities to be able to share and access their academic history in easy but secure ways.

Over the past several years, researchers as well as international organizations have begun to examine blockchain technology as a possible solution to these issues. Blockchain is a decentralized and tamper-resistant digital ledger which has shown good things toward strengthening access control as well as improving transparency. Blockchain has also shown promise in supporting the secure management of educational records. This section explores how blockchain-based access and usage control can be used for educational systems and have a positive impact. This is by improving security, enabling self-ownership of data, micro-credentialing, and cross-institutional collaboration.

Many of the current problems in educational data systems come from their centralized design. Traditional student information systems typically rely on a single institutional database that holds literally everything there is to know for the student. Now, while this approach makes internal operations simpler for a single institution, it also creates several major vulnerabilities. For example, it introduces a single point of failure. If the database becomes compromised from some sort of attack, the institution will most likely lose access to these records. Also, internal manipulation, administrative errors, and data breaches are more of a problem for centralized systems.

Another major issue in traditional educational systems is the lack of interoperability across institutions. For example, if a student decides that they want to transfer from one school to another for whatever reason, there is a high chance that they will experience delays in processing transcripts. Even if it is within the same educational system, records could use different formats or databases which aren't compatible. This then makes what should be an easy record exchange difficult. UNESCO (2022) identifies this as a big problem for educational mobility. This is especially a problem for international students, migrant workers, or those who rely on nontraditional learning pathways. When academic records are kept within institutions, students end up having limited control over their own educational history. This causes them to rely on administrators to provide verification which can take time as many people have experienced. This is sometimes referred to as the student's credential silo problem. It's not the best option so why is it still being used by every institution.

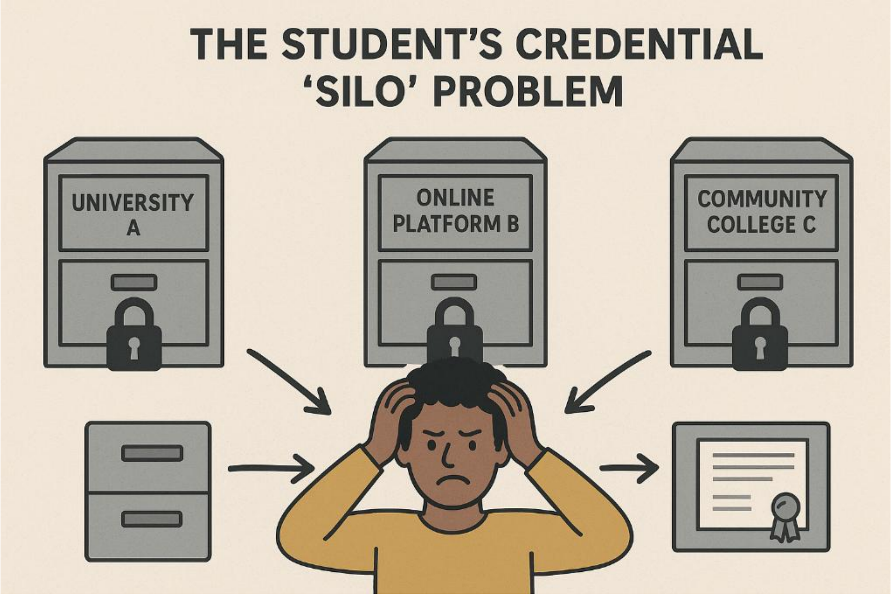


Fig. 4: generated by ChatGPT – Shows the Student credential silo problem

Online learning is becoming a bigger thing year after year, which further exposes these weaknesses. As more students pursue online certificates, courses, and micro-credentials from various institutions and platforms. The problem of verifying these achievements becomes complicated and much more difficult. Traditional systems were not designed to manage distributed learning pathways; I mean how could they have predicted the word turning almost completely online. The world is going to keep moving and isn't going to stop, which means that traditional systems need to adapt with change. The gap between current learning environments and data systems that are outdated shows the need for new infrastructure.

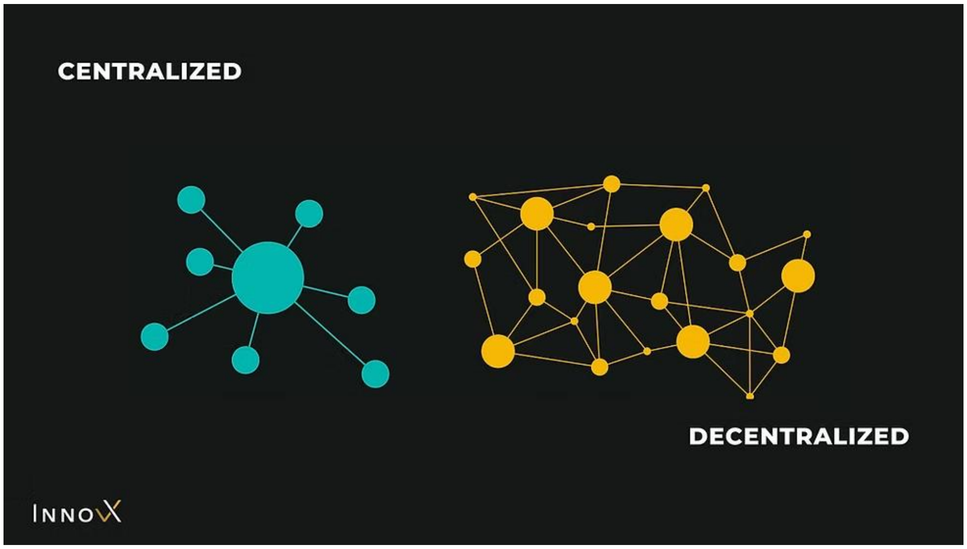


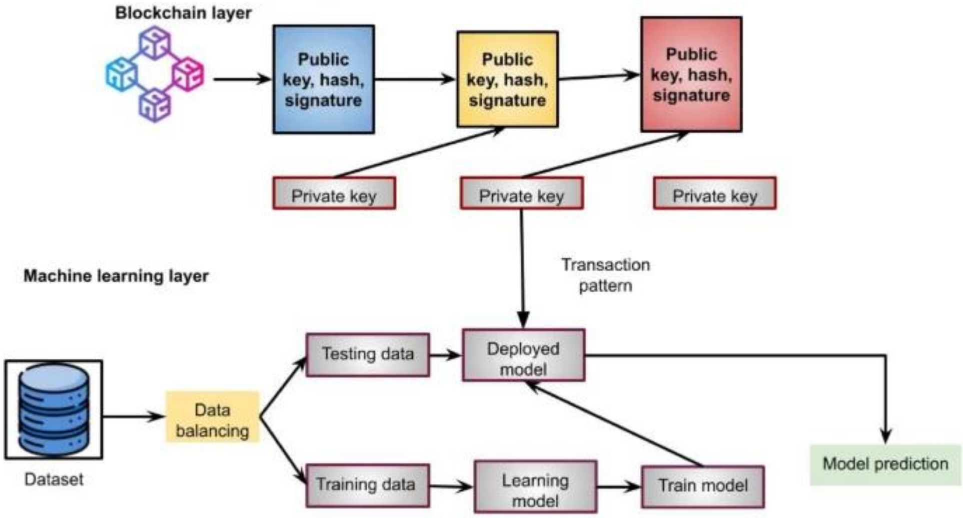
Fig. 5: by Innovx – Shows the difference between Centralized and Decentralized systems

Blockchain offers several characteristics that directly address the weaknesses of traditional systems. Because blockchain stores data across a decentralized network instead of a single database, it eliminates the reliance on a central authority while also reducing vulnerability to internal manipulation. Each record entered into a blockchain ledger is timestamped, cryptographically secured, and practically immutable. Once data is added to the system, it cannot be altered or deleted without leaving a visible trace or relying on a single authority. This makes blockchain ideal for storing sensitive and verifiable information like diplomas, certifications, and transcripts. Basically, it makes it so data can't be tampered with without being able to be uncovered. Everything leaves a trace so no funny business can be done.

One of the most transformative aspects of blockchain is its potential to shift ownership of academic records from institutions to students. According to UNESCO (2022), blockchain creates an environment in which learners can possess a secure, lifelong digital record of their achievements. This record can then be shared instantly with employers or other institutions without waiting for any administrative approval, leading to no wasted time. This allows for maximum efficiency as students are able to send academic records whenever they want without any unnecessary wait times, because who likes waiting.

Moving forward, employers and educational institutions benefit from faster verification processes, which are also more reliable. Instead of contacting a registrar or relying on emailed documents that may be forged, an organization can verify credentials directly on the blockchain. This not only reduces fraud but also increases trust in digital credentials. Going off this information, it seems that blockchain is best for institutions and students.

While blockchain provides a strong foundation for protecting records, the technology must still be combined with robust access control mechanisms to ensure privacy. Educational records often contain personal information which is considered sensitive. Recent research has been focusing on integrating blockchain with role-based access control (RBAC) models to address this challenge. Chinnasamy et al. (2025) presents one of the most advanced implementations of this approach.



Their model combines blockchain with machine learning enhanced RBAC to determine who should have access to various types of educational documents. In this system, the blockchain acts as the secure storage mechanism, while the RBAC layer governs permissions. Everyone receives specific access rights that determine what they can do with the records. These access rights allow for the documents to remain how they should thus keeping their integrity. Meaning that if you should only be able to view it, then you can only view it. If you should only be able to edit, then you can only edit and so on.

The advantage of this structure is that it maintains security while also maintaining flexibility. Students would still have control over who can view their records, but institutions will still be able to enforce privacy rules. On top of that, institutions would also be able to track data use. Because blockchain logs all transactions immutably, any access attempt that is authorized or unauthorized is recorded. Nothing can be hidden as a result of everything being logged. This creates a transparent digital audit trail which increases accountability while also reducing the likelihood of data misuse.

Moving forward, combining RBAC with machine learning enables dynamic adaptation. For example, if there are unusual access patterns that might suggest a security risk, then the system can automatically change permissions or just flag the activity for someone to take a look at. This anomaly detection is more advanced than traditional database permissions. These often require manual updates which uses more manpower and can be inconsistently applied.

The increasing popularity of micro credentialing highlights another area where blockchain can add significant value. Micro credentials consist of small, modular certifications that validate specific skills. They have become widespread in online education, professional development, and corporate training programs. However, the diversity of providers and the lack of standard verification systems create challenges for both learners and employers.

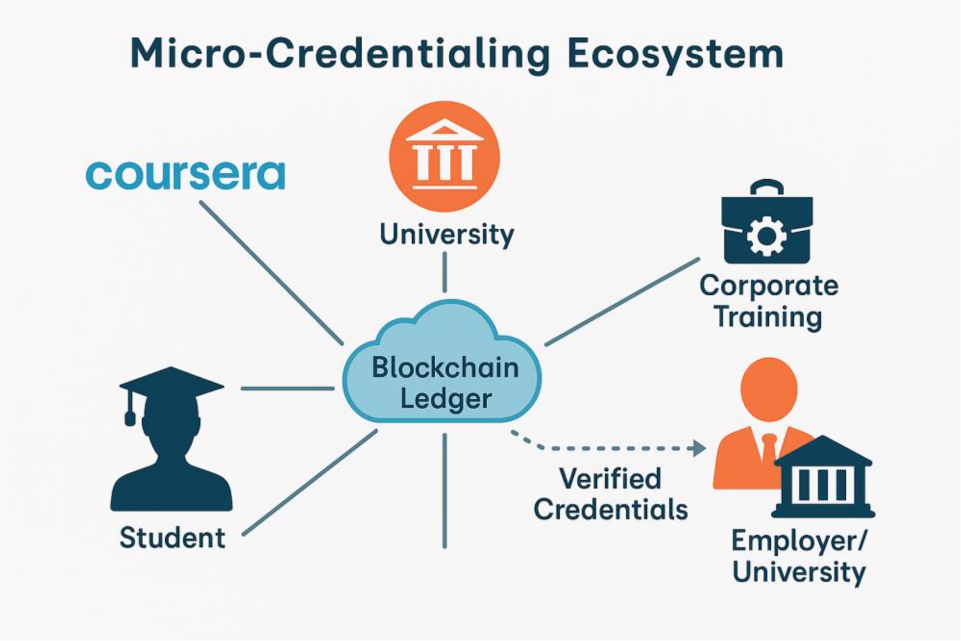


Fig.7: generated by Copilot – Shows how different achievements can be stored in a blockchain ledger and sent to the designated receiver

According to Alsobhi et al. (2023), blockchain is a promising foundation for storing and verifying micro credentials because it provides a secure, tamper proof environment that is not dependent on any single organization. A blockchain-based micro credentialing system ensures that each credential is cryptographically linked to its issuing source. This reduces opportunities for falsification and fraud. Because the ledger is decentralized, you could have all of your credentials in one single place which could be viewed by employers or those that you want to see.

This system also benefits employers, who often struggle to assess the authenticity or relevance of micro credentials. With blockchain in micro credentialing, there is stronger trust than a digital badge or certificate, which can easily be fabricated. Additionally, blockchain supports the needs of people who accumulate skills across a wide range of contexts. As modern careers require continuous upskilling, a verifiable skills record becomes highly valuable, which is also portable. This is especially valuable to those who travel abroad to receive training from different programs and institutions. The ability to have everything in one place and being able to easily access it just makes sense. Why not make everyone's lives a little bit easier?

The educational landscape is moving toward a more interconnected ecosystem, but data interoperability remains a major issue. Lots of institutions use different software systems as well as data formats. This creates a problem for students who move between programs or countries as getting things transferred can be a struggle to say the least.

Ocheja et al. (2022) argues that blockchain provides a foundational infrastructure that can unify these disparate systems. Their review of blockchain applications demonstrates how institutions can maintain autonomous internal systems while contributing to a shared blockchain ledger that stores verified credentials. This approach allows for institutions to remain independent while also allowing universal verification.

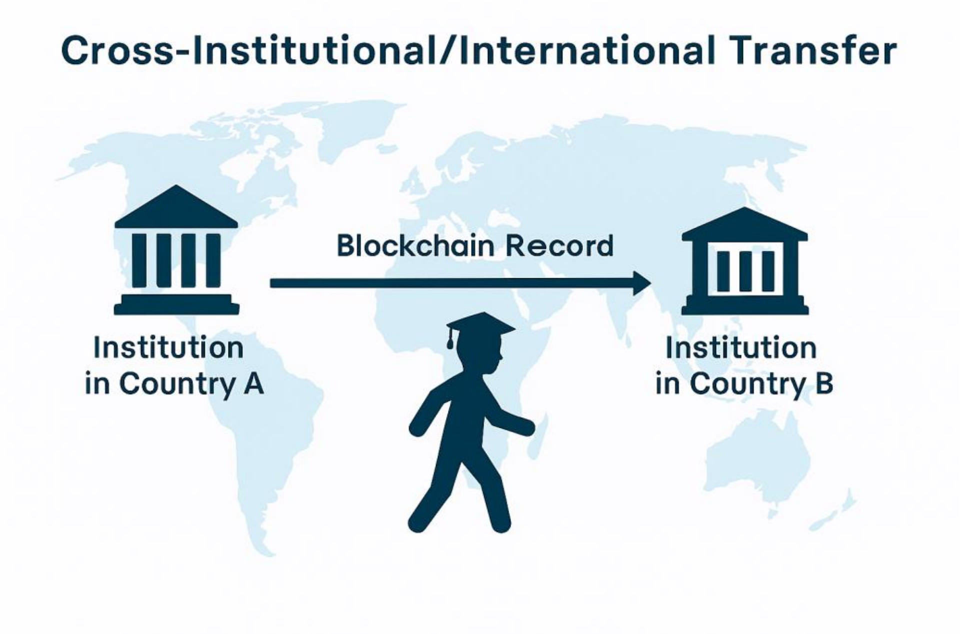


Fig. 8: generated by Copilot – Showing Blockchain Records moving from one institution to another across countries

Cross institutional collaboration also supports broader educational mobility. For example, if a student does some sort of online coursework in one country and transfers to a university in another, then they could present blockchain verified records of their work from the other country. This would eliminate the need for lengthy manual evaluation processes and allow for everything to be seamless. This is particularly important in regions where traditional records may be delayed or possibly vulnerable to being tampered with. Cross institutional collaboration solves most problems.

However, one problem with cross institutional collaboration is the social acceptance of it. It is a big step that institutions would have to take, which would cost them a lot of money to set up the systems as well as manage them. On top of this is the people using these systems, people are used to the way systems are now and can be reluctant to change. This could be from either not trusting the system to protect sensitive records or going with “if it ain’t broke, don’t fix it” mentality. In order to combat this, clear guidelines and pilot programs would be needed as well as overall international cooperation.

Blockchain-based access and usage control has the potential to completely change how educational systems work, all for the better. Its decentralized structure, linked with strong access control mechanisms, offers improvements to systems that most can’t even imagine. By supporting micro-credentialing, enabling cross institutional collaboration, and securing online learning environments, blockchain takes care of a lot of the challenges that are being dealt with now concerning modern digital education. While there are still some kinks that need to be worked out, research over the past several years shows that blockchain could create a more student-centered educational system. Only time will tell, but as educational systems continue to evolve, be on the lookout for blockchain in the not-so-distant future.

4 Government Systems

Government agencies are in charge of keeping very sensitive information systems that contain things like; citizen identification data, national security information, public safety records, and documents that are critical to financial and administrative sectors. The more these information systems grow and connect with each other, the more unauthorized access, insider misuse, credential compromise, and lack of auditability problems increase. Traditional access control models like role-based access control (RBAC) and attribute-based access control (ABAC) were created for isolated environments and do not easily extend to multi-agency government systems. In the scenario access control is extended, it is done so

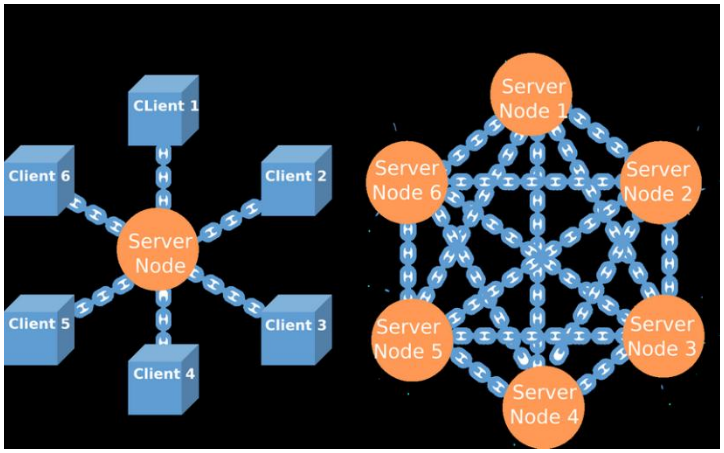


Fig. 9: 1 centralized vs decentralized blockchain architecture diagram (Sutanto et al., 2023)

by attaching conditions and obligations to data use, including time limits, purpose constraints, and continuous monitoring rather than one-time authorization decisions. As (Maesa et al., 2019) explain, “the whole XACML architecture relies on a centralized Policy Decision Point (PDP) that evaluates requests and a Policy Information Point (PIP) that retrieves attributes. This centralized approach makes the system dependent on a single control component, limiting its applicability in distributed or collaborative scenarios where independent parties must verify access decisions without relying on a single trusted authority”. In multi-agency environments, this reliance on central control becomes a very significant barrier to the transparency and ‘inter-organizational trust’ that is needed. Public-sector digital twins almost always span multiple stakeholders, including different agencies, private contractors, regulated industries, and sometimes foreign partners.

On the other hand, blockchain technology offers a new way of doing things that allows decentralized validation, tamper-proof logging, and automated policy enforcement to be used. The following discusses how blockchain can bring government systems to a new level of access and usage control, backed-up by recent peer-reviewed research and federal case studies. The main point is that blockchain can greatly enhance interagency trust in government infrastructures through better transparency, auditability, and so on. At the same time, it does present huge challenges that need to be managed carefully with appropriate governance and implementation strategies.

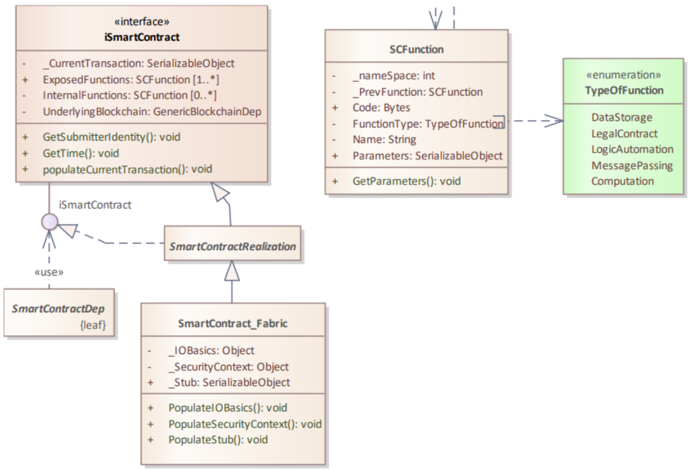
Systems of access control have traditionally depended upon centralized infrastructures where identity repositories, authorization engines, and audit logs are all kept. Such systems are prone to failure as the central servers are potential failure points and could easily be hacked or manipulated by someone within the organization or an external hacker.(Maesa et al., 2019) point out that “the use of centralized ABAC evaluation engines leads to the creation of opaque trust structures that are difficult for independent parties to verify”. In the same way, (Elisa et al., 2018) mention that “e-government systems often rely on duplicated databases, limited authentication safeguards, and inconsistent validation methods, which not only make them attractive targets for cyberattacks but also facilitate the attacks". The problems that centralized systems face become more apparent as government operations go through different agencies, jurisdictions, and service pipelines. Without logging of access that is both consistent and verifiable, it becomes more difficult to ensure accountability. It will then also be harder to carry out investigations or even maintain public trust in the case of a breach.

Blockchain technology, with its decentralization and immutability provides a solution to the problems of traditional access control infrastructures. This is rather than depending on a "single authoritative server, blockchain allows the use of distributed nodes to keep synchronized ledgers indicating all access requests and policy decisions"(Punia et al., 2024). This arrangement can lead to a significant reduction in incidents of unauthorized data modification, prevention of deletion of audit logs, and creation of an environment where access control policies are both enforced and verified consistently.

The article *'Blockchain governance in the public sector'* by (Tan et al., 2022) presents a governance-directed viewpoint that public sector blockchain adoption is very much 'dependent on institutional decision-making, setting of rules, and the mechanisms for updating the system policies. Their model indicates the urgent need for transparent, legit, and participatory governance structures to be in place along with the technical decentralization. The Joint Financial Management Improvement Program article titled *'Harnessing Blockchain in the Federal Government'*(2023) shares lessons learned from a federal blockchain prototype tracking research grant funding as its practical insights. Their results indicate that while blockchain can improve transparency, provide audit trails that are resistant to tampering, etc. It also points out the obstacles concerning cybersecurity, authority-to-operate requirements, and the challenge of achieving data standardization across the government.

The process of blockchain technology adoption is indeed a lengthy one, but its positive effects on organizations, particularly in terms of access and usage control, have already been noted. To begin with, the core characteristic of blockchain that leads to the benefits is its decentralization. The approach diminishes the risks associated with a single authorization server. Now, all the blockchain nodes are validating and checking the access rule, and there is no way that a hacker can control the server, change the permissions, or erase the access logs. Smart contracts, more so, lift the process of controlling usage right through the system. These rules can restrict the ways data can be viewed, used, or changed. For instance, one can set rules that only in certain cases sensitive data can be viewed, and the access can automatically expire after a certain time interval, or document changes can be made only with the approval of all parties involved. The policy enforcement done automatically is less likely to be influenced by human error and has a lower chance of inconsistent application of policies or unauthorized privilege escalation taking place.

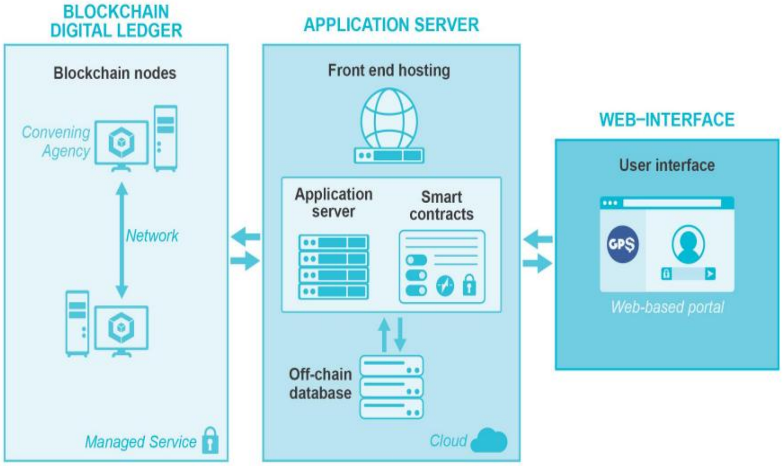
Besides, immutable audit trails are a further step to accountability increase. Blockchain keeps an everlasting record of every access request or policy decision, thus giving the investigators and auditors a complete and tamper-proof record of the system's activity. According to the (JFMIP, 2023) report, “the financial management process with a single drawdown platform based on a blockchain system… provides transparency into the financial process down to the sub-grantee level, standardizes the drawdown process, *eliminates or significantly reduces reconciliations*, and streamlines reporting. Having all the information on the blockchain allows for more consistent and streamlined processes… and provides authorized users with *one integrated and validated data source* that could be used by all parties”. This prototype proves that the use of immutable ledgers results in ‘reduced disagreements among agencies/accurate financial reconciliation, and the establishment of clear visibility into the transaction histories’. This feature is of utmost importance in cross-agency collaborations where the element of shared trust becomes critical.


«interface»
iSmartContract
- _CurrentTransaction: SerializableObject
+ ExposedFunctions: SCFunction [1..*]
- InternalFunctions: SCFunction [0..*]
- UnderlyingBlockchain: GenericBlockchainDep
+ GetSubmitterIdentity(): void
+ GetTime(): void
+ populateCurrentTransaction(): void
iSmartContract
SmartContractRealization
«use»
SmartContractDep
{leaf}
SmartContract_Fabric
- _IOBasics: Object
- _SecurityContext: Object
+ _Stub: SerializableObject
+ PopulateIOBasics(): void
+ PopulateSecurityContext(): void
+ PopulateStub(): void
SCFunction
- _nameSpace: int
- _PrevFunction: SCFunction
+ Code: Bytes
- FunctionType: TypeOfFunction
- Name: String
+ Parameters: SerializableObject
+ GetParameters(): void
«enumeration»
TypeOfFunction
DataStorage
LegalContract
LogicAutomation
MessagePassing
Computation

Blockchain technology, as claimed by Elisa et al. (2018), allows the government institutions to share data securely without the need of duplicating the databases. An example could be blockchain-based digital twins that have been proposed for public health scenarios where real-time data from multiple organizations can be combined in a decentralized way, while access rules and data usage are recorded on a distributed ledger. This gives the possibility of the coexistence of synchronized records between the departments and the control over their separate systems at the same time. Besides, blockchain governance is a major factor of its successful previously suggested adoption. According to Tan et al. (2022), the technical decentralization has to be coupled with the very strong governance structures. This is so that the attributes of being legitimate, just and accountable are not feared to be lost. The agencies must have the same rules for, and the same degree of transparency/standardization in the decisions concerning consensus mechanisms, rule changes, identity management, and administrative power.

Blockchain and its accompanying technology still face several challenges despite the advantages they provide. Gas costs, latency, and scalability remain major limitations, particularly for real-time digital twin applications that require frequent access requests. Scalability is a big issue, and it has been the case for permissioned blockchains that are processing heavy loads of access requests. The same goes for privacy, which is a big concern since the nature of the technology is its immutability. This clashes with the legislation that prescribes the alteration or even the outright deletion of sensitive data. In order to meet the legal requirements, hybrid storage models are frequently used to keep the confidential data off the chain. Operational risks are also incurred due to smart contracts. The JFMIP (2023) report mentions that "smart contract code errors can affect the whole financial operation". It is not easy to fix such errors without requiring coordinated consensus from multiple agencies.

It is advisable for governmental organizations to think about the implementation of permissioned consortium blockchains with an arrangement of multiple departments working as validating nodes. The arrangement provides a middle ground between decentralization and regulatory control. In compliance with this, the government should execute smart contracts for the automatic management of usage control policies and to store less sensitive data through hybrid methods. Nevertheless, government agencies have to set up a common governance framework that will cover changes in rules, standards for identity management, and procedures for consensus. The pilot projects, similar to the JFMIP (2023) prototype, already demonstrate the testing of scalability and the



identification of operational challenges in the process of larger deployment as an effective method.

Blockchain technology can be referred to as the fortress where the access and usage control of the government systems are kept. It will be very difficult for hackers to penetrate. It has been found in some studies that the use of blockchain would yield improvements in the areas of transparency, accountability, and even interagency cooperation as mentioned in this research. On the other side, a well-planned governance structure, system integration, cybersecurity requirements, and operational constraints are among the elements that need to be tackled to have a successful implementation of the new system. As a matter of fact, blockchain is not only able to meet but also surpass the government's trust requirement for information infrastructures as public-sector systems grow in size and complexity over time.

5 Conclusion

The rise in digital learning has made it clear that traditional record keeping systems are struggling to keep up with how education works today. Almost all institutions still rely on these old, centralized databases which make it difficult to transfer and verify records. Blockchain technology has offered a decentralized structure with strong access control which creates a tamper resistant way to store records. It also allows students to share their achievements with ease, thus cutting down wait times. With blockchains support in micro credentialing, the enablement of cross institutional collaboration, and securing online learning environments, this allows for blockchain to deal with a lot of the problems that the current systems can’t. Even though switching to blockchain would require a lot of money as well as cooperation between institutions, the benefits that were talked about far outweigh the costs. As education continues to be more online engaged, the need for a reliable system that makes everyone's lives easier increases.

With blockchain ever growing in the healthcare field and many others. It is important to understand that data is the key to everything related to business. It is very important to keep our information and our customers' data safe. Ensuring that we protect both of us from any and every possible threat. Using blockchain for electric health records has helped improve many systems and methods of ensuring a better and more reliable source of information. Making it easier to find patients' information safer and faster.

The challenges are even more significant in government systems since the agencies deal with very delicate information and must cooperate constantly across all boundaries. Again, the traditional access control tools were not designed for such a complex environment, which is the reason why the agencies are still struggling with problems like unauthorized access, inconsistent validation, and lack of transparency. Blockchain promises a solution to many of these issues by providing the agencies with a common, incorruptible system in which every access decision is recorded and verified among a number of departments. This process helps to create trust and responsibility that have been absent from the large government networks for years.

Despite the fact that blockchain has strong potential to enhance the information-sharing practices of the government agencies, the technology still poses challenges that must be managed. Things like scalability, privacy, and governance are among the issues. However, recent studies demonstrate that the proper implementation of blockchain can lower disputes, enhance auditability, and increase interagency cooperation to a considerable extent. It is definitely something to consider across all boards.

Main Findings	**Recommendations**
Centralized student record systems are vulnerable	Blockchain uses a decentralized system, meaning records are stored on a distributed network
Lack of interrogability between institutions	With blockchain, credentials can move seamlessly between schools and countries
Growth of online learning and micro credential learning is becoming too much for current systems	Blockchain based micro credentialing solves this and allows for each credential to be cryptographically verified and all achievements can be stored on one ledger
Privacy concerns with sensitive student information regarding current as well as blockchain systems	Blockchain with the implementation of RBAC (Role Based Access Control) which allows specific permissions for different people
Centralized access-control systems in governments lead to single points of failures.	Establish a permissioned blockchain with different agencies of the government as validator nodes to abolish dependency on a single Policy Decision Point (PDP).
Government agencies face difficulties in auditability, as logs may be changed, wiped, or not uniformly kept.	Employ unchangeable blockchain audit logs, which ensure that all access requests and policy decisions are documented permanently and can be cross-verified by the different agencies.
Inter-agency data sharing is inefficient due to duplicated databases and inconsistent validation methods.	Utilize common distributed ledgers, which keep in sync records among different agencies, eliminating duplicate databases and allowing instant verification.
Privacy requirements conflict with blockchain's immutability, especially under data-protection laws.	Implement a mixed storage model. Place sensitive personal data off-chain and at the same time keep hashed references on-chain for compliance with privacy regulations.
Patients gain greater control over their health data.	Smart contracts allow them to grant or revoke access to doctors, researchers, or insurers with fine-grained permissions.

Blockchain’s decentralized and immutable design reduces risks of data breaches.	Every access attempt is logged, verified, and visible, ensuring accountability and trust.
Scalability issues, regulatory uncertainty, and high infrastructure costs remain barriers.	Specialized expertise is required to implement and manage blockchain-based systems effectively.
Blockchain facilitates secure data sharing across hospitals, labs, insurers, and research centers	This improves collaboration, reduces duplication, and enhances overall care quality.

References:

1. Bathula, A., Gupta, S. K., Merugu, S., Saba, L., Khanna, N. N., Laird, J. R., Sanagala, S. S., Singh, R., Garg, D., Fouda, M. M., & Suri, J. S. (2024, August 8). *Blockchain, Artificial Intelligence, and healthcare: The tripod of future-A narrative review - artificial intelligence review*. SpringerLink. https://link.springer.com/article/10.1007/s10462-024-10873-5
2. Durneva*, P., Cousins*, K., Chen*, M., Department of Information Systems & Business Analytics, & Cousins, C. A. (n.d.). *The current state of research, challenges, and future research directions of blockchain technology in Patient Care: Systematic Review*. Journal of Medical Internet Research. https://www.jmir.org/2020/7/e18619/
3. Han, Y., Zhang, Y., & Vermund, S. H. (2022, November 24). *Blockchain technology for Electronic Health Records*. International journal of environmental research and public health. https://pmc.ncbi.nlm.nih.gov/articles/PMC9739765/
4. Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2024, October 15). *Permissioned Blockchain Network for proactive access control to Electronic Health Records - BMC Medical Informatics and Decision making*. BioMed Central. https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-024-02708-8

5. Singh, Y., Jabbar, M. A., Shandilya, S. K., Vovk, O., & Hnatiuk, Y. (2025, November 11). *Exploring applications of blockchain in Healthcare: Road map and future directions*. Frontiers. https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2023.1229386/full
6. Sun, J., Ren, L., Wang, S., & Yao, X. (n.d.). *A blockchain-based framework for electronic medical records sharing with fine-grained access control*. PLOS ONE. https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0239946
7. Chinnasamy, P., Subashini, B., Ayyasamy, R. K., Kiran, A., Pandey, B. K., Pandey, D., & Lelisho, M. E. (2025, May 29). Blockchain-based electronic educational document management with role-based access control using machine learning model. Nature News. https://www.nature.com/articles/s41598-025-99683-5
8. Moya, J. A. B. (2025). Zero-knowledge proof-enabled blockchain-based framework for academic credentials. Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2025.00123
9. Punia, A. (2024). A systematic review on blockchain-based access control paradigms. Journal of Cloud Computing, 13(22). https://doi.org/10.1186/s13677-024-00512-0 Quispe,
10. M. A. C. (2025). Blockchain ensuring academic integrity with a degree-verification prototype. Scientific Reports, 15, 8421. https://doi.org/10.1038/s41598-025-89632-3
11. Silaghi, D. L. (2025). A systematic review of blockchain-based initiatives in academic certificate management. Computers, 14(3), 75. https://doi.org/10.3390/computers14030075
12. Cultural Organization. (2022). Education and blockchain. https://www.um.edu.mt/library/oar/bitstream/123456789/108074/1/Education_and_blockchain%282022%29.pdf
13. Alam, A. (2022). Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. In Smart data intelligence: Proceedings of ICSMDI 2022 (pp. 307–320). Springer Nature Singapore.
14. Alsobhi, H. A., Alakhtar, R. A., Ubaid, A., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. Knowledge-Based Systems, 265, 110238.
15. Ocheja, P., Agbo, F. J., Oyelere, S. S., Flanagan, B., & Ogata, H. (2022). Blockchain in education: A systematic review and practical case studies. IEEE Access, 10, 99525–99540.
16. United Nations Educational, Scientific and Cultural Organization. (2022). Education and blockchain.

https://www.um.edu.mt/library/oar/bitstream/123456789/108074/1/Education_and_blockchain%282022%29.pdf

17. Maesa, D. D. F., Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, *84*, 93-119.
18. Corten, P. A. (2018). Implementation of blockchain powered smart contracts in governmental services.
19. Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless networks*, *29*(3), 1005-1015.
20. Maesa, D. D. F., Mori, P., & Ricci, L. (2019). A blockchain based approach for the definition of auditable access control systems. *Computers & Security*, *84*, 93-119.
21. The Joint Financial Management Improvement Program. (2023, December). Harnessing blockchain in the Federal Government. https://www.cfo.gov/assets/files/JFMIP-24-01.pdf
22. Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, *39*(1), 101625.
23. Punia, A., Gulia, P., Gill, N.S. *et al.* A systematic review on blockchain-based access control systems in cloud environment. *J Cloud Comp* **13**, 146 (2024). https://doi.org/10.1186/s13677-024-00697-7
24. Landry, F. (2024, February 21). *Centralized vs Decentralized Systems: Impacts on Business Operations*. Www.innovx.org. https://www.innovx.org/post/centralized-vs-decentralized-systems-understanding-the-businesses-impacts
25. ChatGPT. (2015). ChatGPT. https://chatgpt.com/c/692dd681-29c8-832f-af3d-dca1b4e7f61f
26. Microsoft Copilot: Your AI companion. (2025). Microsoft Copilot: Your AI Companion. https://copilot.microsoft.com/chats/xJh7u8tRu2mPx1hgBErnb
27. Sutanto, Erwin & Mulyana, Rahmat & Arisgraha, Franky & Escrivá, Guillermo. (2022). Integrating Blockchain for Health Insurance in Indonesia with Hash Authentication. Journal of Theoretical and Applied Electronic Commerce Research. 17. 1602-1615. 10.3390/jtaer17040081.
28. Sebastian-Cardenas, J., Gourisetti, N., Wang, P., & Smith, J. (2022, March). *Smart Contract Architectures and Templates for Blockchain-based Energy Markets (V1.0)* . Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-32687.pdf
29. Dodaro, G., Harrison, D., Lebryk, D., & Malague, K. (2023, December). Harnessing Blockchain in the Federal Government. https://www.cfo.gov/assets/files/JFMIP-24-01.pdf
30. Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure

and efficient solution for electronic health records. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *68*(2), 2377–2397. https://doi.org/10.32604/cmc.2021.015354

31. *Blockchain-based Electronic Health Record Market Report 2034*. (n.d.). https://www.cervicornconsulting.com/blockchain-based-electronic-health-record-market
32. Díaz, Á., & Kaschel, H. (2023). Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. Systems, 11(7), 346. https://doi.org/10.3390/systems11070346