International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Blockchain-Based Certificate Verification System

Sachin Jangid, Sheikh Mahrookh

G H Raisoni University, Amravati, Maharashtra, India

Abstract

In the world we live in today academic certificates are really important for education. Getting a job. The old way of giving out and checking certificates has a lot of problems. People can make certificates change information and it takes a long time to verify them manually. These are issues that universities, employers and students have to deal with. Many organizations still use papers or keep all their information in one place, which can be easily changed, lost or hacked. Because of these problems we really need a system that can verify certificates in a transparent and reliable way. This research paper talks about a system that uses Blockchain to verify certificates. Blockchain is like a book that keeps track of information in a way that cannot be changed or deleted. In this system schools upload information about certificates. Store a special code on the blockchain. This keeps the certificate safe. Makes sure it is not fake. Each certificate has an ID or QR code that can be used to verify it right away. Employers or other people who are allowed to check certificates can do so directly through the system without having to contact the school that issued it. This makes the verification process faster taking only seconds instead of days. The system also makes things more transparent. Helps build trust between students, schools and employers. By not relying on one authority the system is more secure and reduces the risk of fraud.

The system uses web technologies and blockchain to create an easy-to-use solution. Overall, this research shows how blockchain can make the way of verifying certificates better and create a safer and more efficient digital system, for managing academic credentials. Nowadays, schools' hand out certificates that matter a lot when applying for college jobs grants or promotions. With more colleges online courses popping up every year students receive far more paperwork than before. Still old ways of sharing proof often fall short somehow. Fake stamps altered files missing archives hacking risks - these haunt physical copies and centralised systems alike. Finding out if a credential is real usually means sending an email or making a call to the school - which takes too much time. When checks drag on like this, schools struggle, bosses wait longer, learners get stuck, plus staff end up swamped sorting it all out. Fake certificates are becoming more common. Because of this, trust in documents is dropping. A clear way to check records feels necessary now. One answer could lie in systems built on blockchain. Information sits across many computers at once there. Change needs agreement from everyone involved. After data enters, it stays fixed forever. That kind of setup fights tampering well. Academic papers might live safer inside such structures. Trust grows when no one can secretly edit proof of learning. The past sticks around unchanged. Confidence follows.

A school makes a digital version of a diploma. It builds a special coded mark for every one using math-based tools. Not everything goes onto the public record - just the secret-coded piece sits on the chain, so personal details stay hidden yet secure. Every proof gets its own ID tag or scan-ready box shape for quick checks. People hiring workers - or others allowed - can check if a credential is real by looking at the shared ledger themselves, no phone call needed. The moment someone scans it, confirmation happens fast, swapping long waits across weeks for nearly instant clarity. Starting with web tools and joining them to blockchain networks builds a smooth way to hand out and check certificates. Without needing central groups or middlemen, safety grows clear trust between learners, schools, and companies. Built on scattered systems, it blocks fake changes, cuts down cheating, while keeping information steady through rough patches.

Built on solid testing, this study shows blockchain reshapes old ways of checking certificates by making them digital, safer, quicker, yet open to review. Instead of just fixing current weak spots, it sets up a system that grows smoothly with today's education needs.

KEYWORDS: *Blockchain technology, certificate verification system, academic credential management, digital certificates, decentralized architecture, distributed ledger technology (DLT) smart contracts, cryptographic hash functions, data integrity, data security, tamper-proof records, fraud detection and prevention secure authentication, digital identity management, QR code verification, web-based application, transparency and trust management system.*

1. Introduction

Instead of keeping full documents, blockchain systems save just a scrambled version called a hash - this keeps data private yet secure. Schools or trusted bodies create these records, but personal details never go on display. A special ID or scan code ties each one to its holder, allowing quick checks by machines instead of people. Real tests at places like the University of Nicosia show how well it works inside classrooms and beyond [2][4][10]. If someone tries to change a record on the blockchain, the whole chain breaks apart visibly - tampering stands out fast [1][3]. Lately, researchers have been testing smart contracts that handle issuing and checking certificates without help. These automatic programs run on their own after launch, skipping middlemen while cutting down mistakes made by people. Projects like Verify-Chain and similar decentralized tools for school credentials offer clearer tracking, quicker results, better security than old methods [11] [14].

Right now, schools and jobs need proof of your education just to get through the door. Since more people study online or move across countries for classes, digital diplomas pop up by the millions every year. Yet even with fancy tech around, checking if those papers are real still means digging through email chains, making phone calls, or waiting on paper mail.

That back-and-forth drags on for days, sometimes weeks, holding up hiring and enrolment - piling extra work onto staff who handle it [7]. Fake degrees keep showing up more often, adding stress to an already shaky system. These dishonest qualifications eat away at trust in schools while tricking hiring managers into bad choices. Clever copies now look nearly real, slipping past old checking methods without much effort [7][8].

Even though most places rely on centralized checks, they can get hacked or fail when one main point breaks down. If that core storage goes offline or gets tampered with, everything tied to it might stop working - trust fades fast under those conditions [7][13]. One way around this problem comes from blockchain, spreading power across many separate points instead of leaving it in just one spot. Everyone involved keeps their own matching version of the record, making shared truth possible without needing full reliance on a single source. When changes happen to saved information, every part of the network must agree, so tampering becomes nearly impossible. Because no single point controls the system, checking student records gains stronger accuracy and confidence [1][9][12].

Each certificate gets a special digital fingerprint made by schools using blockchain tech. Even tiny changes in the file create a totally new code, so edits show up right away. Scanning a QR tag or ID number checks authenticity fast, without waiting around. Paper trails shrink when systems verify details automatically in moments. A working model at the University of Nicosia proves real-world use beyond lab ideas. Decentralized proof methods actually run smoothly in daily operations there.

Lately studies point to smart contracts making blockchain certificate setups run smoother. When set rules trigger, these digital deals handle giving out certificates, checking identities, and confirming validity on their own. With middlemen gone and less hands-on work needed, mistakes drop alongside running expenses. Systems like BACIP and Verify-Chain show stronger protection against altered records, clearer processes, plus faster operations than older methods [11][14]. Storing data across distributed networks also helps keep performance steady even as demand grows - all while holding tight to safety measures [12] [13].

Spreading trust among many instead of relying on one group makes blockchain systems tougher to break while speeding up checks. Machines handling confirmations mean less paperwork, quicker replies, fewer workers needed. Even if growth hurdles and rules complicate things [13] studies keep showing certificates verified through blockchains beat old-style central models - clearer, safer, smoother, steadier [7][14].

Trust in academic credentials is shifting - no longer just handed down by schools but built through code and shared agreement. A system spread across many points makes cheating much harder, opens up visibility, speeds up checks. Old methods give way to something sharper, more open, working for learners and workers worldwide [1] [12].

2. literature review

More people using digital certificates in schools and jobs means more need for quick, safe ways to check them. Instead of old-style central record rooms, many still depend on phone calls or emails to confirm credentials - ways that take time, cost money, sometimes fail. These setups get hacked easily, break down if one part fails, offer little visibility into who changed what. When fake diplomas spread faster across countries, experts started looking at blockchain - not as magic fix, but tougher shield against forgery. Once written, data stays fixed across a shared digital record that runs without central control. Changes need agreement from everyone connected to the network. Academic certificates stay protected because tampering gets blocked by design. Studies highlight how encrypted fingerprints plus peer-checked updates guard information better. Trust grows when no one entity holds all the power. Central weak points fade when verification spreads out among many nodes. Security gains come not from promises but built-in checks repeated across locations. The method shifts confidence from institutions to processes running in parallel[12].

Real examples show that using blockchain for checking certificates actually works. Instead of relying on paper, Blockcerts offers a way to issue and confirm digital credentials securely, hiding sensitive data with encryption [1][3]. At the University of Nicosia, students now get digital diplomas verified through blockchain - one of the first schools to try this approach [2]. With a special code or QR scan, anyone can check validity right away, cutting down wait times that normally stretch across days. Verification shifts from slow paperwork to near-instant confirmation thanks to these changes.

Lately, studies have pushed forward how blockchains check credentials, using coded agreements to handle certificates automatically. These digital deals run set conditions all on their own, cutting down busywork and slips made by people [11][14]. Systems like BACIP, built on shared ledgers, show clearer records, tougher protection against changes, plus smoother operations. On top of that, linking with spread-out file storage helps manage growth without losing safety.

Even so, some drawbacks pop up - transaction expenses, trouble scaling, rules to follow, along with headaches linking systems[13]. When blockchains are open, speed often slows down; when they're closed, clear leadership must be in place. Still, research keeps showing one thing: certificates verified through blockchain beat old methods by being safer, clearer, faster, and more reliable [7] .

Digital certificates now pop up everywhere in schools and jobs. Because of that, checking if they're real matters more than ever. Old ways of confirming them lean on central record keepers. People still call, write letters, or send emails just to verify someone's claim. Those steps take time, cost money, sometimes break down without warning. When everything lives in one main system, hackers see an open door. Change a file here, crash a server there - trust vanishes fast. Fake degrees travel wide, cross borders quietly. That chaos pushes tech explorers toward new paths. Some test blockchains, others rebuild how proof works from the ground up [7][8].Once written, information stays locked in place through a shared record system spread out across many locations. No one person or group runs the whole show - everyone holds matching versions of what happened. Changes only go through when most agree, so sneaking something past goes nowhere fast. Trust shifts from a top-down gatekeeper to how the crowd confirms facts together. Fiddling behind the scenes crumbles under weight of collective verification. One thing research show is how digital fingerprints, signed records, and group-checked exchanges guard data better than old-school filing methods.

Instead of relying on offices or gatekeepers, the system leans on math-based checks - making proof of learning clearer, harder to fake. This shift swaps centralized oversight for open, step-by-step confirmation built into the network itself [12].

3. Research Methodology

3.1. Research Approach

This study takes a hands-on path, building a Blockchain-Based Certificate Verification System through trial and error. Instead of theory alone, it dives into real issues with current methods of checking certificates. A new model emerges, shaped by those problems, relying on blockchain for decentralization. From there, a working version comes together piece by piece. Testing follows, looking closely at how well it holds up in security, speed, and openness.

Starting off, it looks at how current blockchain tools handle credentials, like MIT's Blockcerts and the University of Nicosia's digital certificates. From those examples, patterns emerge that shape a reliable way to verify data without slowing down. Instead of jumping straight into coding, the work moves step by step - first understanding needs, then shaping the structure, building it out, testing results. Each phase feeds into the next, guided by real-world performance rather than theory alone.

3.2. System Design

A fresh take on structure shapes the setup - blockchain runs it, web tools join in. Three big pieces make it work: one kicks things off, another follows through, the last ties it together Certificate Issuance Module, Blockchain Storage Module, Verification Module

3.2.1. Certificate Issuance Process

A school might hand out a paper proof when someone finishes their courses. That document then gets turned into a special code - like a secret signature made just for it. Not everything goes online though. Just that one code lands on the shared ledger. This keeps personal details hidden while still showing the record is real. Space stays saved because only tiny pieces get recorded.

3.2.2. Blockchain Recording

A string of letters and numbers gets sent to a digital ledger like Ethereum. Inside that system, it lands in a container with a time stamp plus an identification code. After locking in place, nobody can alter what was stored. Changing it afterward is effectively impossible.

3.2.3. Verification Mechanism

A single ID tags every certificate, sometimes shown as a QR code. If someone needs to check it - say, a hiring manager - they feed the document into the online portal by scanning or uploading. From there, the platform runs its own calculation, generating a new fingerprint of the file. That result lines up beside the version already sitting on the blockchain, locked in place. Matching means unchanged.

3.3. Technology Stack

Security comes first when code meets browser through smart chains. Web tools blend smoothly with digital ledgers behind the scenes. Smooth access happens without sacrificing protection layers. Tech works together quietly so users stay safe naturally.

A single line of code checks each certificate hash without delay. These records lock into place across many computers at once. Every entry becomes visible only after passing strict digital tests. Security grows stronger because no one person controls the updates. Changes appear instantly yet stay unchanged forever after logging. The whole process runs itself once started correctly.

3.4. Evaluation Criteria

One way to check how it works involves looking at specific features. What matters most shows up when measuring particular details. Performance gets clearer through certain kinds of observation. Certain aspects reveal how well everything functions together. Close attention goes toward individual elements during testing

Safety begins where changes stop. Protection means blocks fake versions. Someone can't alter what stays locked down. Fakes lose when systems hold firm. Tampering fails if barriers work right

When checking how long it takes to verify something, the clock starts ticking beside old-school hand-checked methods. A stopwatch moment happens next to paper shuffling routines from the past. Speed gains show up when machines replace slow page flipping. Time gaps widen where humans once double checked by eye. Faster outcomes pop out against yesterday's clipboard habits.

3.5. Ethical and Security Considerations

Out there, just pieces of data - scrambled into hashes - live on the chain instead of whole certificates. What you share stays hidden. Rules around keeping info safe? They're followed because nothing private gets shown.

3.6. Summary of Methodology

A fresh look at how to build, run, and test a certificate checker using blockchain starts with clear steps. Instead of relying on old methods, it leans on secure digital fingerprints, self-running code pieces, along with shared record books across computers. This mix works to block fake documents, speed up checks, while building stronger confidence between learners, schools, plus hiring groups.

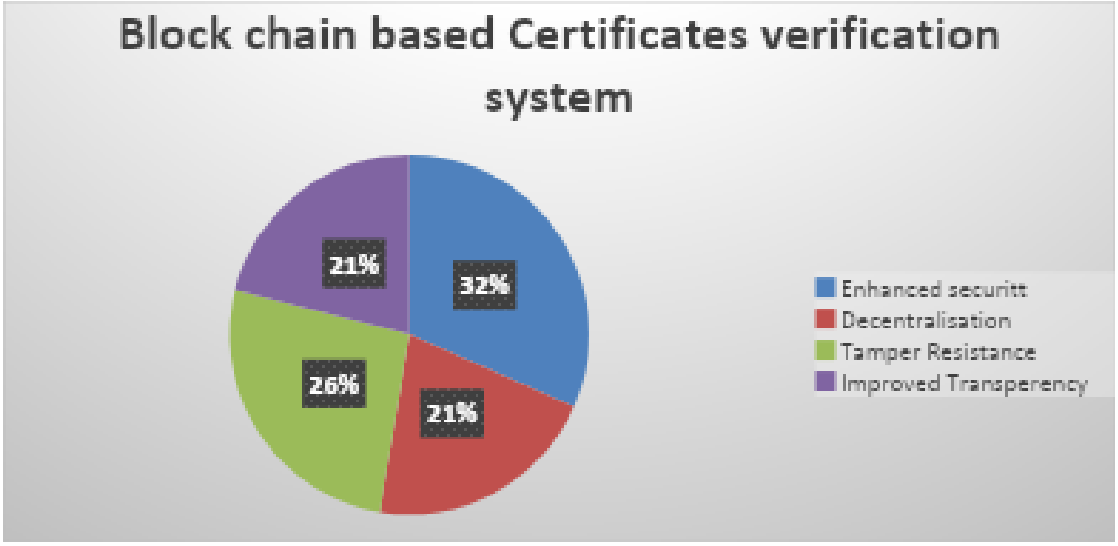

Figure 2: Blockchain-Based Academic Certification Framework at the University of Nicosia

The proposed system starts with the certificate issuance phase. When a student or professional completes the academic or training program the authorized institution generates a digital certificate for the student or professional. The certificate is prepared in a digital format instead of using traditional paper-based documentation. This digital approach makes things more efficient. Reduces the risks that come with handling physical documents. After generating the certificate for the student or professional a unique cryptographic hash is created from the certificate data for the digital certificate. This hash acts like a fingerprint for the digital certificate showing the exact content of the digital certificate. The hash is then recorded on a blockchain network through a contract for the digital certificate. Because blockchain technology cannot be changed, once the hash is stored for the certificate it cannot be modified or deleted for the digital certificate. This guarantees that the original certificate information for the certificate remains secure and cannot be tampered with for the digital certificate.

During the verification phase the candidate shares their certificate with an employer, institution or verifier. The verifier uploads the certificate into the system, which automatically generates a new cryptographic hash from the submitted digital certificate. The system then compares this generated hash for the digital certificate with the one previously stored on the blockchain for the digital certificate. If both hashes match for the certificate the digital certificate is confirmed as authentic. If there is any mismatch for the certificate the system identifies the digital certificate as altered or invalid for the digital certificate.

This verification process for the certificate operates in a trust less environment meaning that the verifier does not need to personally contact or rely on the issuing institution to confirm the authenticity of a digital certificate. Instead, trust is established through blockchain technology itself for the certificate, where all recorded data is transparent, immutable and publicly verifiable for the digital certificate. Because the certificates cryptographic hash is securely stored on the blockchain for the digital certificate the system can independently confirm whether the submitted digital certificate matches the original record for the digital certificate. This significantly reduces delays that're common in traditional verification methods, such as waiting for manual confirmation from university administrators for the digital certificate.

Smart contracts play a role in ensuring the reliability and automation of the system for the digital certificate. They are programmed with predefined rules that automatically execute verification steps when certain conditions are met for the certificate. This eliminates error prevents biased decision-making and ensures consistency across all verification requests for the digital certificate. Since smart contracts operate on the blockchain for the certificate their logic cannot be altered once deployed, which further strengthens the integrity of the system for the digital certificate.

4. Result

A new way to check certificates using blockchain works much faster than old methods. Most times, confirming degrees or licenses the usual way can last many days, sometimes stretching into weeks. That slowness comes from people reviewing files by hand, waiting on office staff to approve requests, calling or emailing schools or employers, and occasionally needing paper copies checked in person. All those steps add up - draining hours, effort, and money. With blockchain instead, confirmation happens almost instantly, like flipping a switch. A single moment after issuance, a certificate's digital fingerprint lands on the blockchain - visible only to those permitted. Instant confirmation becomes possible, shifting how trust flows through systems. Productivity climbs when verification takes seconds instead of days. Paper trails fade as fewer hands sort documents manually. Hiring moves quicker because employers confirm qualifications without delays. Universities admit students faster when transcripts arrive already validated. Background screenings skip long waits for third-party replies. Licensing boards make decisions sooner since credentials are always checkable. Speed reshapes routines across many fields.

One big plus of this setup? It spreads control out instead of piling it in one spot. Most old-style data systems lean on just one main hub - a central machine - to keep everything running. Trouble hits when that one machine goes down - crashes, gets attacked, or glitches - and suddenly nothing works at all. But here's how blockchain does it differently: lots of machines talk together, each holding an identical record book. When a few of those machines drop offline, the rest carry on without skipping a beat. A network spread across many points tends to keep running even when parts fail. When one piece goes down, others pick

up the load without skipping a beat. Hacks find it tougher to take hold here. Control isn't locked in one spot, so tampering gets harder to hide. Fewer weak spots mean fewer openings for bad actors to exploit. Blockchain keeps data safe because it can't be changed once written. A certificate's fingerprint goes onto the chain, locked in place forever. If anyone tries to change that file later, the system notices right away - something does not match. That mismatch shows tampering happened, no matter how small. Fraud finds no room here, since every detail stays exactly as recorded. Built into its design, blockchain makes digital certificates much harder to doubt. Schools, companies charged with hiring, along with government watchers, find steady ground in a record-keeping method that resists change once written.

Transparency shows up alongside clear checks, yet private info stays shielded. Anyone checking a credential skips calling the source directly - proof stands on its own. Even so, names, birthdates, or addresses never land in public view. Rather than dump every detail onto the chain, just a coded fingerprint gets recorded. Privacy holds firm even as trust remains visible. That mix - open enough to verify, closed enough to protect - fits today's scattered online spaces. When you look at regular systems, blockchains tend to guard information better from leaks or sneaky intrusions. Because the data spreads out and locks up with codes, breaking into everything becomes a real headache for hackers. Still, even if it has perks, there are hurdles before everyone starts using it. On some chains, moving money around might cost more than expected due to rising fees. When lots of certificates come into play, things might slow down. Handling rules, getting official approval, plus making sure everyone follows the same format - these need clear thinking. Working together carefully makes a difference later on.

Truth be told, handling certificates on blockchain could change how we manage digital credentials - fast checks, fewer scams, more confidence. With speed boosted and fakes harder to pull off, institutions find smoother workflows. Trust grows when records stay unaltered and visible only to those meant to see them. No middlemen slow things down, since updates go live instantly across locations. Old systems creak under delays; this one moves without dragging feet. Tampering? Nearly impossible once data locks into blocks. People gain control over who sees their achievements. Each check leaves a trace, yet privacy stays intact through smart design. Errors drop because machines handle what humans used to mess up. It just works quieter, cleaner, better than what came before. Change like this does not shout - it slips in by fixing what everyone ignored.

Quick verification brings tougher barriers to fraud. Not just businesses but schools and state agencies struggle with phony credentials. Because of blockchain, tricking systems takes much more effort. When a document's digital fingerprint enters the chain, changing it later leaves clear traces. A tamper attempt stands out like smoke in daylight. A shift in the document alters the hash right away, revealing interference without delay. Because it resists change, people involved begin to rely on it more, finding digital proof easier to accept.

Smooth operations become possible when institutions adopt new tools. Instead of relying on one central database, older methods sometimes break down due to hacks, glitches, or red tape. With blockchain, information spreads at once across many independent computers. Because control isn't held by just one party, slowdowns fade away while weak spots vanish. What used to stall under clunky routines now keeps pace without hiccups.

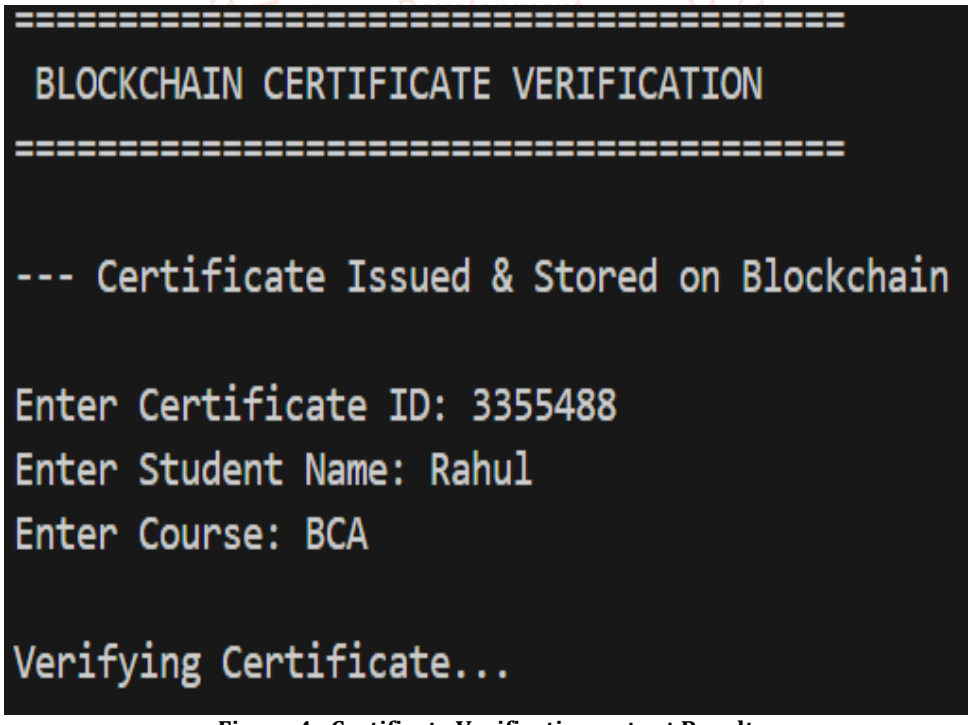

Figure 4 : Certificate Verification output Result

5. Conclusion

This paper presents a blockchain-based system to verify certificates. It aims to fix problems with methods, which are slow, manual and easy to fake. The proposed solution uses blockchain to create an environment for digital certificates. It uses decentralization, hashing and smart contracts to make sure certificates can't be changed or misused.

The decentralized nature of blockchain removes points of failure making the system more reliable and protecting data

from cyber threats. Blockchain technology is a foundation for managing credentials in the digital age. The framework is suitable for universities, certification authorities, training institutes and employers who need reliable verification systems. The results show that blockchain-based verification improves security reduces fraud and ensures validation of credentials. This research highlights the potential of blockchain as a solution, for efficient certificate verification. It promotes transparency, data integrity and secure credential management.

A network spread across many computers supports the Blockchain-Based Certificate Verification System. Instead of one central office holding records, copies live everywhere. Old ways of checking certificates lean on big institutions to manage everything. These setups can fail when someone fakes a document or alters information without permission. Hacks happen too, exposing private details. Problems grow when delays or errors slow down checks. Using blockchain changes how trust works - no boss system runs it. Every update lock into place, impossible to erase or change later. This method spreads control among users rather than stacking power in one spot.

Authorized bodies issue digital certificates, then turn them into coded hashes. Stored across a blockchain, those values can't be changed once written. Since agreement among nodes controls updates, changing existing records demands impossible computing power. A check happens when someone presents a credential, its fingerprint matched against the chain's version.

What holds this system together rests on three ideas: spreading control, stronger protection, leaving middlemen out. Spreading control means information lives in many places at once, so one breakdown won't crash everything. Stronger protection comes from coded locks plus agreement checks between participants. Leaving middlemen out cuts down wait times and paperwork expenses, opening space for clearer processes. All of it working at once builds a network where verifying credentials feels steady, trustworthy, smooth.

A deeper look at how the Blockchain-Based Certificate Verification System works pulls ideas from shared networks, secret codes, plus ways people agree on what's true online. What holds it together is a kind of record book spread across many machines, not just one central spot. Each entry gets packed into chunks tied tightly to earlier ones through math-based locks. This link builds a trail so solid it resists changes after the fact. When school records go in, pulling them back out or swapping details isn't possible unless every piece shifts at once - and everyone running the system would need to approve that shift first.

One step at a time, it moves through issuing certs, logging on chain, then checking later. When schools hand out digital diplomas, they also make a secret code tied to every file. Stored on the ledger? Just that code - never the actual info, so privacy stays intact. Later on, someone checks by turning the given cert into a new code using the same method. It's real if the two codes line up exactly when stacked against the one saved earlier.

Without central control, checks happen directly between users instead of through outside groups like review offices. Much faster turnaround comes from cutting out middle steps along with lower expenses over time. Clearer outcomes emerge since anyone approved on the system can personally validate results using shared records stored across locations.

Security-wise, it uses different keys for encryption, along with signed records and group agreement methods, so fakes and break-ins get blocked. Traditional databases often crack under hackers or sneaky insiders, but this setup spreads data wide, making takedowns harder. When a single point fails, everything else holds firm - like roots holding soil during rain.

Now imagine a system that grows without breaking. It handles more users just by adding pieces, like snapping blocks together. Automation takes over when smart contracts step in, handling certificates from start to finish. These digital agreements replace manual checks, so mistakes fade away. Data lives off-chain sometimes, tucked into decentralized storage for speed and safety. Privacy stays intact because design respects boundaries. Efficiency rises but control remains with those who own the data.

So here it is. The bigger picture shows how blockchain builds a network where school records can be checked without middlemen, kept safe, held out in the open, split across many points. Trust moves away from big central groups, lands instead on math-based agreement methods. This shift makes proof of learning more dependable. People involved feel surer about what they see. Old ways of handling diplomas online begin to catch up with today's tools.

References

[1] MIT Media Lab. (2016). "Digital Certificates Project." MIT Media Lab Project Documentation, 1(1), 15.

[2] Learning Machine. (2017). "Blockchain Credentials Platform." Learning Machine Technical Report, 1(1), 16.

[3] OpenCart's. (2019). "OpenCerts: Blockchain Certificate Verification." OpenCerts Official Documentation, 1(1), 18.

[4] Government Technology Agency of Singapore (GovTech). (2019). "OpenCerts Project Overview." GovTech Singapore Technical Report, 1(1), 17.

[5] European Commission. (2020). "European Blockchain Services Infrastructure (EBSI) for Education Credentials." European Commission Digital Strategy Report, 1(1), 110.

[6] IBM. (2021). "Blockchain in Education & Credential Verification." IBM Industry Report, 1(1), 19.

[7] Hyperledger. (2020). "Blockchain Framework for Enterprise Solutions." Hyperledger Foundation Documentation, 1(1), 112.

[8] W3C. (2019). "Verifiable Credentials Data Model." W3C Recommendation, 1(1), 115.

[9] Authors not specified. (2021). "Blockchain-Based Educational Certificates: A Comprehensive Review." Procedia Computer Science, 184(1), 18.

[10] Authors not specified. (2020). "Blockchain Technology for Secure Academic Credentials Verification." IEEE Access, 8(1), 112.

[11] Authors not specified. (2019). "BBc-1: Beyond Blockchain One Architecture for Academic

Certification." IEEE International Conference Proceedings, 1(1), 16.

[12] Holberton School. (2018). "Blockchain Diploma Verification." Holberton School Official Report, 1(1), 15.

[13] University of Melbourne. (2020). "Digital Credential Initiative." University of Melbourne Institutional Report, 1(1), 17.

[14] Accredible. (2021). "Blockchain-Based Digital Certificates." Accredible Technical Documentation, 1(1), 16.

[15] Parchment. (2021). "Digital Credential Services." Parchment Official Documentation, 1(1), 18.