ALISTER INC

The Use of Blockchain within Evidence Management Systems

Authors and Researchers: Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright

Co-authors: Rebecca and Jeff Neithercutt, Curtis Darnell, and Dr. Kris Lea

Edited by Katherine Neithercutt

Contents

Abstract

This paper focuses on effectively using blockchain technology within the Law Enforcement chain of evidence, which can be considered a type of supply chain for evidence collection. The authors and researchers of this paper are using the terms "supply chain" and "chain of custody" interchangeably. Alister Inc. is introducing a blockchain-based evidence management system to alleviate the problems the traditional chain of custody has, including loss of evidence, theft, tampering, and worse, manipulation of evidence within the evidence management system.

With the use of blockchain technology, improperly targeted police officers and defendants can be protected from chain of custody issues that can lead to wrongful termination for officers and worse, false imprisonment for defendants. This paper will describe the particular challenges of storing evidence on a blockchain, and provide an efficient solution. David Billard points out some of these challenges in his white paper [1]*Tainted Digital Evidence and Privacy Protection in Blockchain Based Systems,* which the authors and researchers of this paper will be responding to.

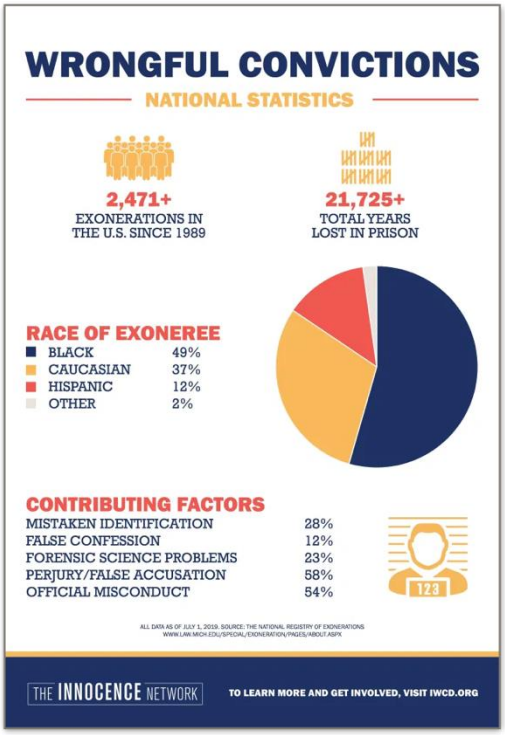
The technology and security behind the use of blockchain will be described using actual cases from past events. This will clarify how the Blockchain of Evidence system from Alister Inc. and the LOCARD.EU (https://LOCARD.EU) project could be invaluable to the supply chain of evidence, and how LOCARD.EU and Alister Inc. are collaborating to improve the integrity and transparency of evidence collection worldwide. Researchers from Alister Inc. will utilize the Blockchain of Evidence system to illustrate the concepts behind the importance of this type of system within societies around the world.

[1] Billard, David. (2020). Tainted Digital Evidence and Privacy Protection in Blockchain-Based Systems. Forensic Science International: Digital Investigation. 32. 300911. 10.1016/j.fsidi.2020.300911.

Introduction: The Problem Today

A conservative estimate gathered from various news and scholarly resources suggests that approximately 20,000 people in the U.S. are falsely accused, convicted, and incarcerated every year. The use of various sources and the approximation of the number is required because no single entity collects validated information about exonerations due to false convictions, and even if they did, we cannot yet know about the cases which were never exonerated.

Of the estimated 20,000 persons falsely accused, convicted, and incarcerated in the US alone, exonerations are few and far between. Exonerations granted by contributing factor include 28% convicted due to mistaken identification, 12% gave false confessions, 23% were due to forensic science problems, 54% are attributed to official misconduct, and 58% are due to perjury and false accusation (Source: The Innocence Project. More than 100% due to some cases having multiple contributing factors.[2])



In fact, according to the National Institutes of Justice, "The most significant number of wrongful convictions in which forensic science is considered a contributing factor is attributable to eyewitness misidentification and official misconduct."[3] Many people effectively lose their entire lives to false imprisonment as the average term served by those falsely convicted was 10 years. That's a decade in the life of a brother, sister, father, mother, colleague, or student who will not be allowed to contribute fully to society once falsely convicted of a crime. Even after release, convicts struggle throughout their lives to gain and keep opportunities those without a criminal history are provided.

[2] https://www.law.umich.edu/special/exoneration/Pages/ExonerationsContribFactorsByCrime.aspx
[3] https://www.ncjrs.gov/pdffiles1/nij/250705.pdf

Also, false convictions have led to a breakdown of trust between the members of the current US criminal justice system and the people of America. This has occurred in part due to the high volume of violent attacks, false evidence, and false testimony by "trusted" agents of Law Enforcement, leading in part to the severe political turmoil seen today.

Unfortunately, corrupt police officers sometimes successfully promote to leadership positions, and entire departments can end up with policies, procedures, and status quo systems in place that regularly tamper with evidence in cases against good police officers and defendants who are targeted. In fact, in the study from Texas State University, "Case Deconstruction of Criminal Investigative Failures" (National Institutes of Justice 2014-IJ-CX-0037), the authors discovered that when police malfeasance was detected, "However, unlike the response to an airplane crash, the criminal justice system typically makes little effort to understand what went wrong. Such failures tend to be ignored and systemic reviews are rare. As a consequence, important necessary procedural changes and policy improvements may not occur."[i]

We know that good police officers want, and in some cases need, a way to stop this type of evidence tampering from being used against innocent individuals, particularly in police systems with corrupt officers in ranking positions.

Blockchain, a mathematically based and proven distributed ledger system historically used predominantly for cryptocurrency, has shown promise in the supply chain arena, particularly in the tracking of goods.

Many researchers have also built theories about its potential use in the justice system to track evidence within the chain of custody. Researcher David Billard states in his white paper *Tainted Digital Evidence and Privacy Protection in Blockchain Based Systems*[1] that it is not practical to use blockchain for the chain of custody in storing evidence due to multiple legal and information technology system challenges. His main concern was how to remove evidence from the blockchain if it is deemed inadmissible or invalid for any number of reasons.

The authors, researchers, and co-authors of this paper have re-examined Billard's paper and have found ways in which blockchain can assist in the tracking of evidence, even if the evidence is later deemed inadmissible or invalid, with proper configuration and use of the blockchain service. We will also discuss how in some cases blockchain can assist in providing

accountability and transparency to those working in law enforcement when chain of custody issues with evidence arise between collection and presentation in court.

According to the Netflix documentary *How to Fix a Drug Scandal*, more than 34,000 falsely convicted citizens were convicted due to tampered evidence and a lack of accountability of those working within the evidence management system. According to Edward Baumel, blockchain researcher from California State University, Sacramento, "What it boils down to is, the current system is not capable of detecting changes to the evidence while it is in transit from location to location,"

In the Netflix documentary *How to Fix a Drug Scandal*, segment 38:30 of Season 1, Episode 3, ACLU Massachusetts Legal Director Matt Segal stated that, "there wasn't even a process in place to identify the (possibly tainted) cases ... The fact that it was so hard just to figure out the list of the people whose cases were processed by (the lab technician) gives you a sense of this chaos. What was going on in there? It should have been possible to walk in that lab and press a button on a computer and generate a spreadsheet of all her cases with all the information you need to correct those on day one. It took years even to figure out what cases she worked on. How is that possible?"

Though Billard claims that the blockchain system requires extensive measures to ensure evidence can be removed if deemed inadmissible or invalid after collection, there are several ways blockchain can be used to alleviate the problems listed in Matt Segal's statement above.

Understanding the Functionality of Blockchain within Evidence Tracking

Distributed Ledger Technology is described as, "The distributed ledger database is spread across several nodes (devices) on a peer-to-peer network, where each node replicates and saves an identical copy of the ledger and updates itself independently and immediately upon any change. The primary advantage is the lack of central authority (a single ledger where all transactions are tracked). When a ledger update happens, each node constructs the new transaction, and then the nodes vote by consensus algorithm on which copy is correct. Once a consensus has been determined, all the other nodes update themselves with the new, correct copy of the ledger.[3][4] Security is accomplished through cryptographic keys and signatures.[5][6][7]"

In the Blockchain of Evidence (BoE) system, by Alister Inc., each deployed evidence management system member (Police or Evidence Agency) becomes a distributed Node, responsible for assigning each user a user ID, password, and Multi-Factor Authentication (MFA) biometric function before being allowed access to upload to the blockchain. All other users have read-only access and can view what is on the blockchain at any time without authentication. This gives defendants, defense attorneys, judges, citizen review boards, and the general public equal access to proof of the integrity of all submitted evidence, and only authorized users (Officer, Evidence Tech, Prosecutor) the ability to update the blockchain, which cannot be done anonymously. Because no victim/witness information is included in official Evidence Logs, no private information is released. A typical evidence log entry is, “Witness 2 Recorded Statement” or “Victim 3 Video Statement” preventing privacy of those not accused from being violated.

Providing this unprecedented transparency into the supply chain of evidence will reduce officer and investigator responses to general inquiries about cases, freeing them up for further public service. It can also be limited in cases where exposure could compromise the investigation or where release of just the fact that a piece of evidence exists is problematic. This will also decrease the amount of time it takes for the evidence portions of complex cases to be written as the information will be available for upload into the report directly, instead of having to be manually entered one piece at a time.

Understanding blockchain technology may seem intimidating at first glance. However, with some basic terminology, the functionality of a distributed ledger blockchain system can be easily grasped. The most important concept with distributed ledger technology is the concept of trusted Nodes. In a private blockchain every trusted entity and department that installs the software and adds evidence blocks to the blockchain is a Node. Every node can view all the information and data contained on the blockchain in real time. In the following explanation, Blockchain of Evidence (BoE) will be described for its theoretical use in the chain of custody as a blockchain-based evidence management service.

When describing Blockchain of Evidence specifically, an analogy that can be used to help understand the way it functions is our already widespread and generalized use of secure, tamper resistant chip-and-pin-based credit cards. Each credit card number is assigned to a specific and unique user. During a modern-day credit card transaction, after inserting or swiping

the card, a Personal Identification Number (PIN) is required to verify and authorize a transaction. The card number and authorizing pin are then sent to the merchant's payment processor. Once each transaction is authorized, it is given an authorization code which is transmitted back to the merchant. The transaction and authorization code are then recorded on the bank statement or receipt, and each transaction recorded on the bank statement is marked with the date and time and location of when and where the transaction occurred.

BoE's technology works very similarly in regards to tracking evidence in that it provides security, integrity, transparency, and accountability. When officers use BoE on their assigned digital smartphone, they are able to capture metadate currently available, but not collected. "Metadata, or detailed information about a particular piece of digital data such as a picture or document, provides an additional layer of encoded information within the main file. Examples of metadata are time stamps, geospatial information, or even copyright information. Often, the inclusion of metadata is automatic on mobile devices though there are options to disable encoding. Such data have clear evidentiary value for investigations but can also tap into privacy concerns, given the range of additional information. Additionally, this data can be altered either directly or remotely by a knowledgeable technology consumer—as a result, investigation protocols will need to become more sophisticated as strategies shift focus onto metadata validation." [ii]

Users of BoE will use their digital smartphone when they interact with the BoE app that can be easily carried to crime scenes (analogous to the secure credit card in the example above.) They will log in to this app using a username and password, as well as a second form of authentication (MFA) that must be biometric in form; fingerprint, facial recognition, etc. (analogous to the card number and PIN in the above example, only more secure.)

The smartphone, user identification, password, and second form of authentication the officers are given are assigned *only to them,* so that when they login to the BoE private blockchain network within the app all activity they conduct is directly and immutably attributed to their specific credentials. Also, because the MFA is biometric, even if someone were to get the Officer's phone surreptitiously they could not access the system to enter evidence without being immediately detected, though without a specific case and suspect in mind, doing so would seem futile as well.

When an Officer or Evidence technician arrives at a crime scene, their verified credentials and biometric MFA will allow the authorized individual to access their account on the BoE network, where they can take digital photographs of the evidence item(s) they are collecting via the BoE app on their smartphone. This captures only the "state", or condition the item is in at the time it is gathered. It is impossible to convert a physical item to a digital one, however, the "state" an item is in at the scene when collected is extremely important to the validity of the case.

The BoE app will then add the GPS-based location of the evidence, badge number, case number, weather information, or any other metadata added to the system by the user to the photograph file header. BoE then hashes the photograph to immutably capture the state of the evidence, record notes, and log their findings into their account, where their own personal "evidence receipt" or digital ledger will be created (analogous to the bank statement in the example above.)

The credentials they use on their department-issued smartphone will also be used on the BoE website to attribute evidence they collected from a crime scene to their Police Report or evidence record. These credentials will only allow the officer specifically assigned to the account to access whatever evidence they've collected while on the job.

This creates the equivalent to the "purchase" within the credit card analogy and is used to symbolize when an officer collects a piece of evidence via the blockchain system. Each piece of physical evidence is labeled using a tamper-evident Radio Frequency IDentification (RFID) barcode label and then hashed through encryption with the other metadata (case number, badge number, location, etc.) before the hash is uploaded to the blockchain, hosted in the blockchain service provider[4] cloud. Because the RFID tag is uniquely numbered, assigned to that specific user, and "tamper-evident" it would be extremely difficult for someone to remove and replace the exact RFID tag on a piece of evidence without detection,

[4] Blockchain service provider is a full stack SaaS platform that's hybrid enabled (cloud and local storage) and designed to simplify the process of building consortia and deploying private blockchain networks. The service provides a "permissioned" implementation of the Ethereum protocol, whereby member participants operate with authenticated identities backed by digital certificate chains.

and, they would have to do it at exactly the same date/time/location as the original RFID tag was captured in the "state" photograph that was hashed at the scene.

Only the hash is uploaded, and the digital photograph and the physical evidence remain in the custody of the collecting officer or evidence technician, to be booked into the secure evidence storage location for that agency. Each block in the chain relies mathematically on the block in the chain behind it, so removing or modifying any block in the chain is immediately evident and detected by all Nodes (all other agencies with the blockchain system installed,) as their copies of the distributed ledger will no longer match.

For evidence technicians or lab workers that use desktop or laptop computers, they use the BoE website for entry with their user name, password, and a second form of authentication (and the private network will be in affiliation with an agency or lab department that the officer works for).

The "hash", in relation the piece of evidence that was recorded, will be listed on the officer's personal evidence "receipt" and can be transferred directly into the evidence page of their police report. Each time the officer creates a new evidence "receipt", the evidence "receipt" is placed within its own "block" creating a chain of digital blocks, hence the name "Blockchain". This immutably links the collecting officer to the evidence and metadata collected, immediately and forever.

As each Police Agency deploys blockchain, they establish a network of trusted Nodes and receive the latest copy of the blockchain ledger. As each piece of evidence is hashed and captured a new block is generated and uploaded to the blockchain copy at all Nodes simultaneously and immediately, making it impossible for only one agency to ever be able to modify the blockchain of evidence without immediate detection by the others, as their copy won't match, which will break the chain. This is a private, federated blockchain, so all users are credentialled and known.

For example, when the evidence is collected by the officer, he/she takes the photo to capture the "state" of the item and the BoE app generates the hash, which will show up on the officer's digital evidence receipt and is stored in the blockchain, while the photo will be stored in digital evidence. If the evidence in the example above is narcotics, then the narcotics will be sent to the drug lab and the hash will be uploaded to the blockchain. This immutably records the

packaging, weight, time/date/location, and any other metadata added to the BoE app during the hashing process, making recreation of the exact "state" of the evidence when recovered highly improbable at a later date.

Once the evidence is logged into the BoE system, each person subsequently handling the piece of evidence has to scan the label (the tamper-evident RFID tag) with their own BoE app or website to show the transfer of custody and recapture the new "state" (condition) of the evidence. When physical evidence is booked into the Police Evidence storage locker, it gets hashed and captured again. When the Police Evidence room Technician moves it to a shelf or other storage location from the locker, they hash and capture the state of the evidence again using their BoE app. When it gets picked up to be taken to the lab for processing, the transferring technician uses their BoE app to hash and capture the "state" again. When it arrives at the lab for testing the lab technician uses their BoE app to hash and capture the "state" of the evidence. The evidence is never insecure or out of the custody of the authorized chain of evidence users, and the hashes are stored transparently on the BoE blockchain.

This recapturing of the "state" of the evidence at each chain of custody transition point does not in itself prevent tampering, loss, or damage of the evidence, but what it does improve is the likelihood of reporting of impropriety by the person receiving the item, as they can immediately compare the "state" of the item when the person delivering it to them originally captured it, to the "state" it is in when they are now taking custody of it, allowing them the opportunity to report any differences and identify where in the chain of custody the "state" of the evidence item changed.

This dramatically improves on the current chain of evidence, where the person picking up or receiving the evidence has only the "reliability" of the person delivering it to use as a gauge for whether to trust that the evidence hasn't been tampered with in transit. Now, any visible change in the packaging, color, weight, age, or other distortion of the evidence from the last captured "state" hash will be immediately evident to the receiver, and they can refuse to accept it and report the problem immediately, instead of receiving it and not knowing what condition it was in when the person delivering it to them originally took custody themselves.

Any movement of the evidence without hashing and capturing the "state" of the evidence again will invalidate the chain of evidence and make the evidence integrity questionable in court.

This creates a digital trail from the collection of evidence at the crime scene, all the way to court, and makes it possible for judges, prosecutors, defense attorneys, and investigators, to see where the evidence was recorded to be, what "state" it was in at each handling point, and who was in charge of it at each stage of its journey.

Unlike the traditional transaction recording system within a bank, however, if an evidence "receipt" is removed, or changed, the next block after it will no longer mathematically verify, and the blockchain will be invalidated. In other words, there will be a "break" in the chain. If the chain is broken, the blockchain system will mark it as being changed by documenting the change to a new block (fork) and all nodes will be notified.

Because the change is documented at each node, it will be easy to track where the change or loss occurred. If a piece of evidence is changed, all users in the chain can see which law enforcement worker (Officer, drug analyst, forensic anthropologist, etc.) touched it last. This creates an environment within law enforcement that will make accountability of employee behavior much easier to track, and disproving evidence mishandling allegations easier to defend. (see Figure 1).

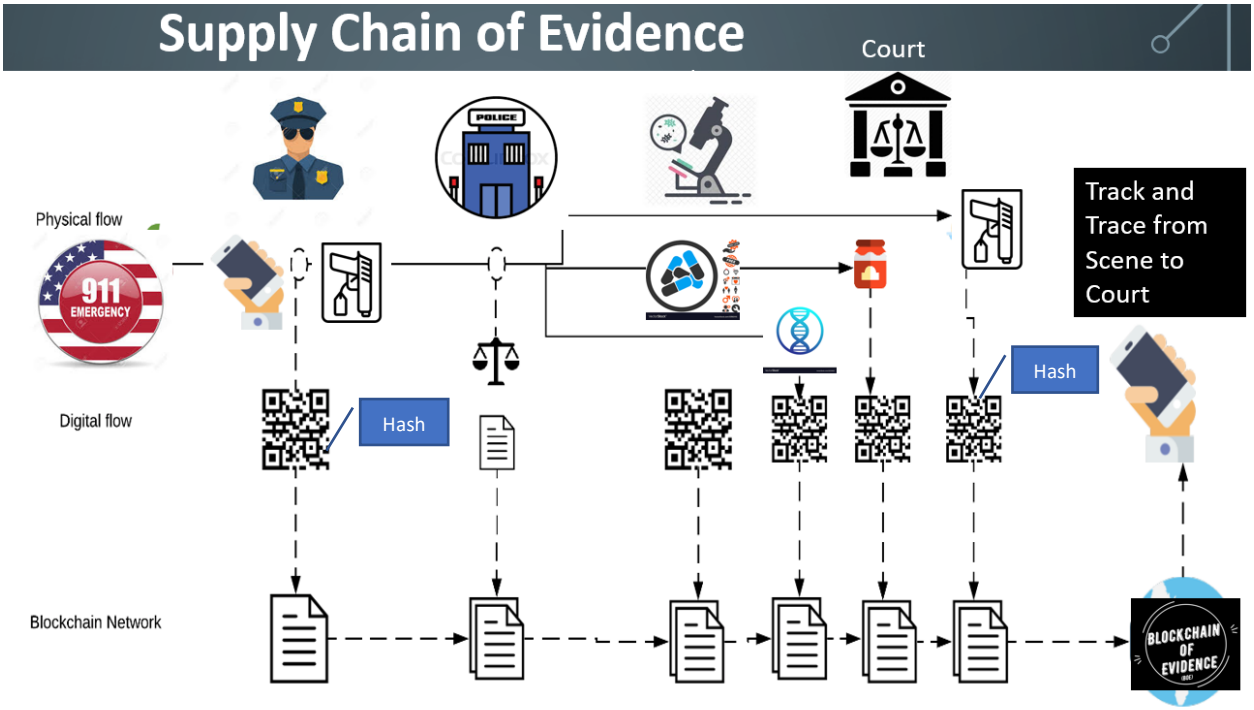


Figure 1- In the diagram above, the process begins when an authorized user arrives at a crime scene after a 911 call or Officer-generated activity. They locate a gun and photograph it in place to capture its "state". Then they attach a tamper-evident RFID tag to the gun and capture the state with another photograph. This creates a file that is then sent to the personalized blockchain network of their employing police department. Once

the evidence has been captured and uploaded to the blockchain network, the digital flow (see diagram) will launch by tracking the hash created when photographed. The digital hash contains metadata and information about the collected evidence and is encrypted using mathematical algorithms proven worldwide. The hash is then added to the blockchain network. One may be confused on how the hash alone in the blockchain can uphold the integrity of the evidence, but when the evidence is in any way changed, a different hash will be formed and displayed on the public ledger. To further improve the integrity of the blockchain, a copy is stored and immediately updated at every police agency using BoE every time a piece of evidence is added by an Officer.

According to the article by David Billard, blockchain causes a storage problem when a piece of evidence stored *inside the blockchain* is later deemed inadmissible or invalid by a court. This argument is flawed, simply due to the probable lack of understanding of how the US court system works. In the United States, the chain of evidence never changes, even if a piece of evidence is deemed inadmissible or invalid. If a piece of evidence is deemed inadmissible by a judge, the prosecution and defense are instructed not to introduce that piece of disallowed evidence before the jury, and the jury is none the wiser. The disallowed evidence is never actually removed from the evidence storing authority until it receives a legal and authorized "purge" or "destruction" order.

In this blockchain system, because the evidence itself is never stored on the blockchain, an order of invalidity or inadmissibility would result in no change to the blockchain, as only the hash is stored there, and the Prosecution or Defense would then never propose the disallowed evidence in front of the jury, nor would the Jury be able to glean any information about the disallowed piece of evidence even if the blockchain were disclosed, as all they would be able to see is the hash value, not the evidence itself.

Further, as to "evidence in a blockchain", a physical item cannot be placed within a digital system, as it is physically impossible to do so. However, a physical item can be indelibly marked with a number to label the item in question (RFID tag), and then the "state" of the item is captured in digital form (photographed and hashed). This allows the physical item hash to be recorded in the blockchain system, adding integrity to the evidence logged. The digital hash of a physical item is derived from a photo containing the RFID label to capture the "state", which is attached to the evidence itself, and the hash of that "state" photo is then placed within the blockchain, not the actual physical or digital piece of evidence, which is stored securely as it is

now. This is a hash of this document at one point in time:

(cd777acd99f2dd874d07de3a1812a8bff4c5e919d0c0f30d4a320b244a91efb8)

Note that while the document's validity and creation state and timestamp can all be verified with this hash, nothing about the article is visible simply by viewing the hash.

The Usefulness of Blockchain to Correct Social Injustices

There are several examples of cases that blockchain might have helped resolve if put into place. A recent example involved the murder of a young boy, about which the interviewed investigators stated, "no one knows how he died, or why" (Marissa Perlman, *CBS News* 2020). Several issues within this case have to do with official agencies not knowing with any certainty where evidence was taken, nor what was done with it after arrival. The case began on January 11th, 2020, when a young boy was found dead near his Northern California home. A few days later an autopsy was performed, and a toxicology report was said to have been collected as well, but the pathology report was reportedly never given back to the investigators in charge of the case.

After six months of investigating the case, the investigating officers still had little information regarding the location of the toxicology report or the cause of death. As of August11th, 2020, the boy's cause of death has still not been revealed by police, who claim the Coroner's office has not released it. Meanwhile, the Coroner's office claims the consulting pathologist hasn't provided them the autopsy report, and the consulting pathologist states they gave the autopsy report to the police, who state they never received it. There have been no updates regarding the case since then and the boy's family are suffering terribly. Digital tracking using blockchain could have described exactly who had what and when.

Another example of the imminent need for blockchain to track evidence comes from New Mexico, where an ex-deputy sheriff was found to have hoarded over 70 pieces of evidence from his previously assigned cases. Though the purloined pieces of evidence were found recently, the ex-deputy had not been with the force since 2014. By the time the evidence was discovered, the "statute of limitations" for charging the deputy with stealing them had passed. This means the case essentially "expired," and the ex-deputy could not be prosecuted for his crimes. This also

means the missing evidence was not available to other investigators attempting to solve the crimes the evidence was linked to.

Blockchain systems could have provided authorities information about the unauthorized removal of the evidence immediately upon it occurring as the ex-deputy would have had to update the "state" and sign out the evidence to remove it. This could have resolved this issue, as supervisors would have been able to keep him accountable for the evidence he collected, and a regular audit would have shown items were collected at the scene that were not turned in to the evidence room. In other words, an investigation could have been initiated immediately upon the evidence being removed, and the ex-deputy likely would not have gotten away with "not completing his duties" (Madrid 2020).

Currently, most law enforcement agencies are not able to communicate effectively or securely with each other and/or within their staff and facilities. There is no existing system that provides all agencies a secure way to pass information to and from most counties or the state, and there is currently no way to keep track of missing or delayed evidence beyond wet-ink signatures and paper logs. Even digital logs won't record when evidence is missing unless someone changes the status in the evidence management system to "Missing". Blockchain can help mitigate this pain point for law enforcement.

In the case of the boy's death related above, the lack of communication between the police department, forensics, the consulting pathologist, and the coroner, has only added to the already existing mistrust between law enforcement and civilians. The longer it takes to solve this case, the easier it is for evidence to get lost or manipulated along the way, or for the killer to strike again. Had this case been using a blockchain type system, the record of the evidence would have been added to the block as soon as it was obtained, notifying each agency to take the next step in the investigation or allowing them to follow up on any delays.

Evidence tampering is already very rare in most agencies, and it would become practically impossible to do without detection with the use of blockchain. Every time something changed about the evidence, the "state" would be captured and hashed with a timestamp and a Gps-based location and then uploaded to the blockchain, and all departments on the blockchain would know exactly where the evidence was when last verifiably stored, and its "state", at any given time.

Having intentionally tampered evidence in a case is more common than the researchers writing this paper had thought, as evidenced by, “Elizabeth A. Johnson, a former director of the DNA laboratory at the Harris County medical examiner's office in Houston, (who) said the task would be daunting. "A conservative number (of tampered evidence) would probably be 5,000 to 10,000 cases," Dr. Johnson said. "If you add in hair, it's off the board." (CSI Is a Lie, APRIL 20, 2015).

Most modern Police agencies use evidence management systems such as Records Management System (RMS) Evidence and Property modules to keep track of evidence, but many departments cannot afford the cost of these systems. BoE is cheaper to implement, is user friendly, and can overlay onto existing systems already implemented within police departments. Blockchain use improves the integrity of RMS Evidence and Property module by adding immutability and transparency to the system, and the departments don’t have to change anything about their existing systems to install it.

The Similar Use of Blockchain in Other Industries

Blockchain technology is already being used for supply chain tracking to track shipments of goods worldwide, proving that it is an excellent resource and that it would be easy to transfer the same process to the supply chain of evidence.

Walmart has already implemented this kind of technology to track E. Coli tainted Romaine Lettuce. In the article *In Wake of Romaine E. Coli Scare, Walmart Deploys Blockchain to Track Leafy Greens*[iii], the author explains that products as simple as romaine lettuce can be tracked in seconds from the shelves of a store, all the way to the hands of the worker that plucked it from the ground. This process used to take weeks, and was sometimes impossible. With their new blockchain deployed, and distributors and farmers on-board, Walmart knows the source of all of their lettuce, and they can track each head of lettuce down to exactly what farm and farmworker had the possible contamination of E. Coli. This makes it so that Walmart only has to recall the packages of lettuce from that specific farm, picked by that specific worker, reducing the total product loss to only the offending packages, and reducing the chance for other

customers to get sick or die from the contamination during the weeks or months the current tracking system takes to operate.

In a recent update, Walmart Canada reported, “its deployment of what it calls "the world's biggest industrial IoT/blockchain roll-out" has reduced shipping discrepancies by 97%.”[iv]

Blockchain could also be used in the meat industry. For example, contaminated meat at restaurants could be more easily identified, located, and recalled. Faulty batteries within cell phones could also be more easily identified, located, and recalled. It could be used in the automotive industry to track cars, car parts, products, and sales. In the health industry, a blockchain type system could be used to keep track of high-risk pharmaceuticals, making it easier to track opioid possession among patients and staff, and overages in prescriptions from specific physicians and pharmacies. Keeping track of medical procedures and practices is also possible with blockchain.

Blockchain will be useful not only in the US for evidence tracking, but world-wide. LOCARD.EU plans to implement a blockchain of digital evidence system within Europe in 2021. The LOCARD.EU system is, “a next-generation, European based platform to process digital evidence through blockchain technology” (LOCARD.EU). The goal of the LOCARD.EU collaboration is to “elevate the level of security in Europe”, and “provide Law Enforcement Agencies, Judicial Authorities, and private companies (with a tool) to manage digital evidence easily”. LOCARD.EU is based in the EU, and Alister Inc. is based in the US, but because of their collaboration blockchain for evidence collection will likely soon be in use in every country and continent around the world to ensure a safer, trusted justice system world-wide, reducing false conviction rates and cutting court backlogs.

The Usefulness of Blockchain in Court

Theoretically speaking, when blockchain is used in a court setting, a list of the evidence hashes from each case will be available to the prosecution, defense, and judicial authority, along with the physical evidence proposed for use in each case. The evidence will support the case and the blockchain will add integrity by further enhancing the validity of the evidence. This will allow all parties an easier time determining the validity and facts of said case. As a result, it may

increase the speed with which the judge can determine the outcome of the case, and it may decrease the chances of having irrelevant or damaged evidence admitted into the courtroom.

Frivolous cases will be dismissed early and an increased amount of evidence will be proven relevant and validated, making less viable evidence obvious. It may even be possible to have the defense and the prosecution stipulate the validity of the evidence ahead of time, reducing the need for some trials, thereby reducing overall court costs and backlogs.

This will ensure there will be a faster, more consistent and secure justice system because blockchain does not allow for as much human error. In a court setting, an individual accused of a crime would be able to compare a current hash against the evidence collected at the scene to verify the integrity of the evidence and ensure nothing has changed.

If the judge rules the evidence to be inadmissible, the evidence can be disallowed from court without altering the blockchain. There will be no need to amend the blockchain or change the hash. Because no human-readable information is included in a hash, no one would be able to glean private or unintentionally released information from the list of hashes that are used to check the integrity of the evidence, allowing the hashes on the blockchain to be visible to the public if desired and configured for public view. This involves training evidence collectors to only label the hashed files with generic terms, such as “Recorded Statement of Witness 1”, “Video from Victim 2’s home”, “Photograph of Vehicle 2”.

Without the use of blockchain, the justice system is more vulnerable to human error and intentional tampering, without the ability to track and record evidence sufficiently to prevent false convictions. In a way, using blockchain will allow for the justice system to add proof of the validity of the evidence, allowing the evidence to “speak for itself”. Blockchain is better suited to effectively track and monitor the condition and preservation of evidence by having the security of the blockchain without having the element of human error or criminal intent.

Conclusion

In conclusion, the use of blockchain to enhance the integrity of evidence in the criminal justice system is vitally important and just makes sense. It can be an inexpensive and comprehensive solution allowing agencies to continue using all of their existing products while removing most elements of human error and criminal intent from the process.

Alister Inc. and LOCARD.EU plan to implement blockchain in the chain of evidence to help restore the public trust in the criminal justice system. Through blockchain, the verified tracking of evidence within different law enforcement agencies will be possible. Only hashes proving the physical evidence "state" will be registered within the system allowing for better and faster processing and more digital storage space. The attribution of hashes to physical pieces of evidence will allow for immutable tracking of evidence from scene to court, and this system will allow for inadmissible evidence to be easily dismissed in a timely manner.

Through the unfortunate cases that have been described above, the authors and researchers from Alister Inc. hope to give their readers a firm grasp of the importance blockchain will have within the justice system, and the many ways it will support the fight toward a more just and accurate criminal evidence tracking system. Accurate evidence with proven integrity is critical in maintaining due process within the judicial system worldwide, and using blockchain to track it can help decrease the instances of political turmoil due to false arrests and convictions.

If we fail to correct this systemic problem within our criminal justice system, we will all suffer the loss of many hard-working, honest, and falsely accused Americans who might have been an excellent Police Officer, or the next great Doctor, Lawyer, Researcher, or Inventor. We simply can't afford not to change, and blockchain in the supply chain of evidence is the change we need to implement.

References

Barone, Emily. "Exonerations: Falsely Accused Freed at Highest Rates." *Time*, Time, 2020, time.com/wrongly-convicted/.

Cummings, Brandi. "Q&A: Placerville Police Discuss Roman Lopez's Suspicious Death." *KCRA*, KCRA, 20 Feb. 2020, www.kcra.com/article/qanda-placerville-police-discuss-roman-lopezs-suspicious-death/31008060

Farmer, Brit Mccandless. "The Opioid Epidemic: Who Is to Blame?" *CBS News*, CBS Interactive, 21 June 2020, www.cbsnews.com/news/the-opioid-epidemic-who-is-to-blame-60-minutes-2020-06-21/.

Friedersdorf, Conor. "CSI Is a Lie: Forensic Investigations Are Overdue for Reform." *The Atlantic*, Atlantic Media Company, 26 Apr. 2015, www.theatlantic.com/politics/archive/2015/04/csi-is-a-lie/390897/

Lustbader, Sarah, et al. "Spotlight: 'A New Wave of Prosecutorial Transparency'." *The Appeal*, The Appeal, 7 June 2019, theappeal.org/spotlight-a-new-wave-of-prosecutorial-transparency/.

Madrid, Associated Press | Salina. "Police: Ex-New Mexico Deputy Hoarded Lost Evidence in Home." *KFOX*, KFOX, 31 July 2020, kfoxtv.com/news/local/police-ex-new-mexico-deputy-hoarded-lost-evidence-in-home.

NA. "Today Is Wrongful Conviction Day." *Mid-Atlantic Innocence Project*, MAIP News, 2 Oct. 2019, exonerate.org/wcd2019/.

National Institutes of Justice, "Wrongufl Convictions and DNA Exonerations: Understanding the Role of Forensic Science", April, 2018, NIJ Journal issue no. 279, https://www.ncjrs.gov/pdffiles1/nij/250705.pdf

Neufeld, Peter Neufeld. "How Many Innocent People Are in Prison?" *Innocence Project*, The Innocence Project, 12 Dec. 2011, www.innocenceproject.org/how-many-innocent-people-are-in-prison/.

Perlman, Marissa. "Social Media Sleuths Hope To Crack Unsolved Death Of Placerville Boy Roman Lopez." *CBS Sacramento*, CBS Sacramento, 30 Jan. 2020, sacramento.cbslocal.com/2020/01/30/social-media-unsolved-death-placerville-roman-lopez/.

Schwartzapfel, Beth, and Hannah Levintova. "How Many Innocent People Are in Prison?" *Mother Jones*, Smart, Fearless Journalism, 12 Dec. 2011, www.motherjones.com/politics/2011/12/innocent-people-us-prisons/.

Union, European. "LOCARD.EU." *LOCARD*, EU, 2019, https://LOCARD.EU

https://en.wikipedia.org/wiki/Distributed_ledger#cite_note-3

https://en.wikipedia.org/wiki/Distributed_ledger#cite_note-Shaan-4

https://en.wikipedia.org/wiki/Distributed_ledger#cite_note-5

https://en.wikipedia.org/wiki/Distributed_ledger#cite_note-6

https://en.wikipedia.org/wiki/Distributed_ledger#cite_note-7

---

[i] https://www.ncjrs.gov/pdffiles1/nij/grants/254340.pdf
[ii] https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf
[iii] https://corporate.walmart.com/newsroom/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens#:~:text=coli%20in%20romaine%20lettuce%20and,from%20eggs%20to%20breakfast%20cereal.&text=Today%2C%20Walmart%20and%20Sam's%20Club,the%20farm%20using%20blockchain%20technology.

[iv] https://www.techrepublic.com/article/walmart-canada-iot-blockchain-system-nearly-eliminates-shipping-discrepancies/