trokt | blockchain

Democratizing Digital Truth

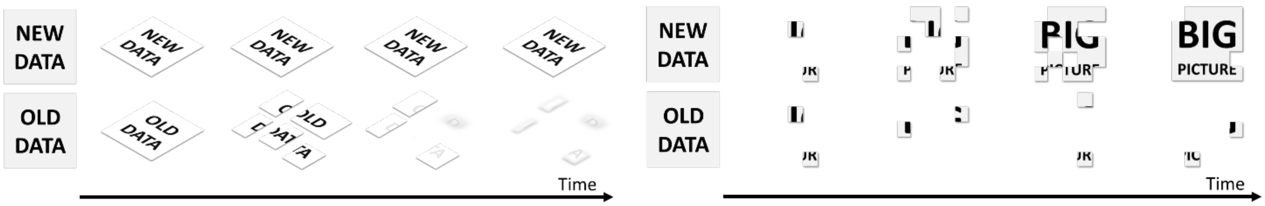
White Paper v2019.1.0

Table of Contents

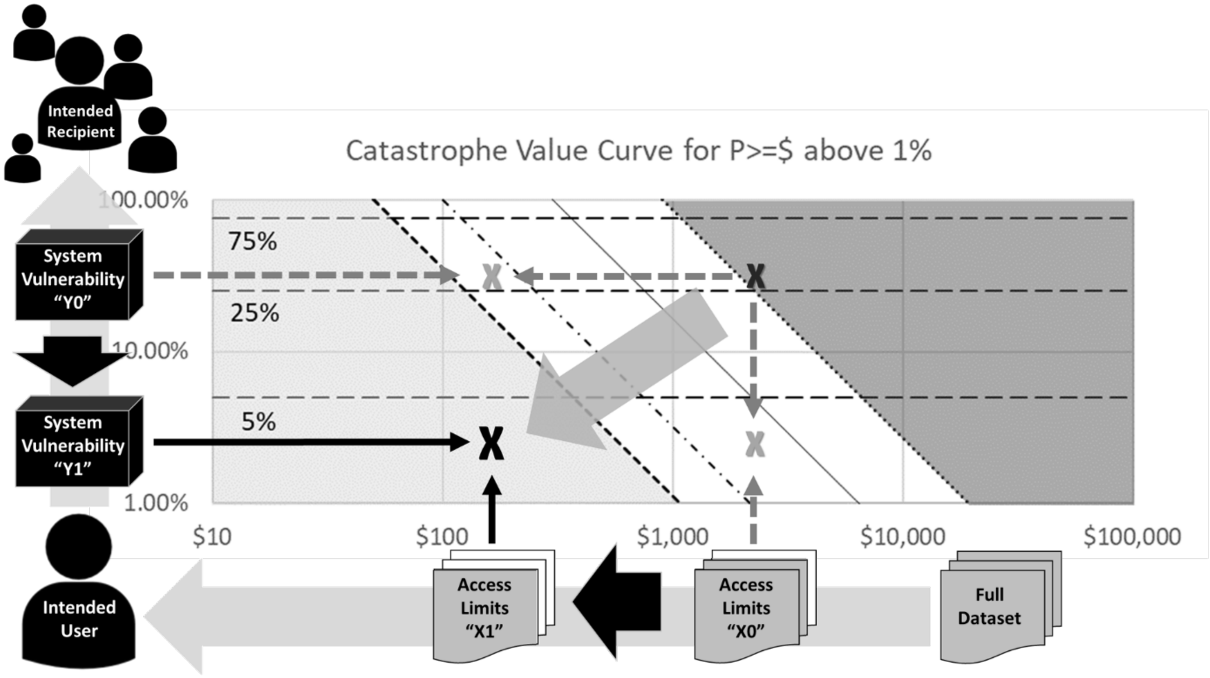
Block 1: Preface

Information is not linear. Nor is transparency uniformly valuable. Yet a just society requires community ownership over anchors of shared truth, around which we can construct our context. These anchors of shared truth, without constraining data structure or context, are the underlying value of Trokt: ***distributed data validation for our modern legal systems***.

Our society's legal systems are grounded in the information gathered from its data, and this ground is shifting. Digital data is no longer as fragile or opaque as old, physical data. Where old data fades, new data replicates infinitely without degradation. Where old data remains isolated, contextualization of new data unearths inexplicit trends that could not be previously seen. Yet inexplicit trends that originate by contextualizing non-degrading data do not automatically reflect societal truths. Too often, misalignment between data weight and quality leads to injustice.



The frameworks for how our legal systems validate and protect this new data are fundamentally transforming. The most recent data management framework to gain traction in the legal community is a risk-based model that is built on over half a century of acceptance in the petrochemical, nuclear, and aerospace communities (Draper, C.H., and Raymond, A.H., Business Horizons, 2019), where systems are optimized for breach risk relative to implementation cost by either reducing penetration rate or fractionalizing data associations.



After a generation of moving towards various versions of cloud and shared database concepts, these new frameworks are responding to data breach and privacy violations that demonstrate the danger of mineable data. Even when data is anonymized or encrypted and personally identifiable information is isolated, contextualization means fragments can now be rebuilt into reflections of the omitted keys to gain insights that economically replicate a traditional breach. These types of replicated breaches occur, for example, when communities are small enough that the conclusions of anonymized data can only be talking about one or two people; a spouse unexpectedly receives an errant, encrypted email from a divorce attorney, thereby revealing the data most desired to be secret; or cryptocurrency transactions allow individuals to identify nefarious actors based on their direct or shared interactions.

Trokt has spent over half a decade building and managing process tools for legally sensitive collaborations that ensure truth by minimizing human operational errors in siloed yet connected datasets. It is now turning its attention to the problem of "distributed truth."

Block 2: The Problem

Modern legal service providers, tools, and processes almost exclusively codify agreements in documents. Whether starting from an online template, a locally executed word processing tool, or scanned from a physical document, these documents are stored everywhere from local hard drives to commercial cloud storage, enterprise servers to email folders. The ubiquitous use of these tools during dispute resolution, agreement development, and document drafting is horribly inappropriate from an operational security perspective.

Ironically, though, ***these fragmented storage methods are the safest way to protect the legal industry's data from a global perspective.***

However, distributed storage has one major flaw: how does someone prove that a document has not been altered? If two parties have two different versions of the same document, and each claims its version of the document is correct, how does the court know which version is true? ***How do individuals prove truth in a digital world?***

The sheer number of participants controlling so many different forms of data using so many disparate systems that rarely communicate effectively FUNDAMENTALLY PREVENTS the kind of data breaches seen with Facebook, Target, or Ethereum Classic. Because so little data is interconnected in the legal industry, breaches are naturally firewalled at the boundary of that isolated user's system. This is where Trokt provides a unique solution to the legal industry where current blockchain concepts are just exacerbating the current problems of:

- <u>Inaccessibility.</u> Current blockchain tools require so much intellectual and operational setup by the end user that it is unlikely one will ever hear a Senior Partner in a law firm tell an Associate: "go here, do this, and bring back the confirmation that you used our blockchain tool correctly." ***The legal industry sees most blockchain solutions as black boxes.***
- <u>Centralization.</u> Current blockchain technology is typically built into platform processes or operations that result in the creation or colocation of centrally stored metadata. This centralized data could be directly applied to the public ledger, thus magnifying the cost of a blockchain related breach when compared against a traditional intrusion. ***The power of distributed storage is limited when centralized metadata is at risk of contextualization.***
- <u>Rigidity.</u> Most blockchain applications are unable to practically weight the relevance of uncertain data. An inability to erase or apply meaningful quality weightings means data requirements are often more precise than a human operator's inputs. ***Blockchain applications are typically an example of fitting people to tech, not fitting tech to people.***

- Complexity. The need to create, manage, and isolate the seed and wallet data driving most blockchain applications is difficult for the average user to consistently manage. ***The setup complexity of most blockchain applications means human operators will employ risky shortcuts that reduce their security benefit.***
- Discoverability. The protection afforded by publicly tying transactions to generalized user details allows all user transactions to be grouped even if the content of the transaction is unknown. ***The trends identifiable in a public ledger are often more valuable than the details of any specific transaction represented.***
- Artificial Incentives. Blockchain solutions that integrate a cryptocurrency Token into its workflow often create markets that require the buyers to simultaneously be sellers. ***Cryptocurrency incentives that do not fundamentally separate the sources of revenue and the direct beneficiaries of revenue growth are rarely sustainable.***

Trokt is now facilitating the creation of the community-owned truths that legal systems depend upon by allowing users to control the context of how a non-technical individual validates fragments of his or her own distributed data. To this day, the most reliable form of document validation in our digital world is an antiquated industry facing near extinction at the hands of the Fourth Industrial Revolution: Certified Mail from the U.S. Postal Service.

Since its creation in 1955, Certified Mail has become both a financially important product for the U.S. Postal Service and one that fulfills a critical legal and business need for American citizens. It has grown to be the largest of the Ancillary Services offered by the Postal Service.

Certified Mail is widely used by Americans with approximately 58 percent of people having used it for either personal or professional mailings. *- USPS*

Certified Mail accounts for over half of all Ancillary Services revenue, bringing in more than $670 million in FY 2016. *- USPS*

Originally proposed as an offshoot of the Registered Mail system, Certified Mail was an innovation that provided a way for citizens to send critical business and legal documents with similar visibility and accountability, but at a lower price. Over time, citizens' trust in Certified Mail has made it an essential communication channel between citizens and government, as it is used to transmit documents such as tax returns and a variety of important public notices. By including tracking and verification that a letter was sent and delivered, Certified Mail provides customers peace of mind about their most important mail items and offers added assurance and security for sensitive documents.

Due to these advantages, Certified Mail has served at least two critical legal functions. First, Certified Mail validates delivery. Parties in legal proceedings frequently must prove that they mailed relevant documents to other parties and that those documents were received. The mailing receipts and delivery notifications that Certified Mail provides allow it to be used as prima facie evidence in legal proceedings. Before its introduction, there was no nationwide agreement about what mail products met this legal standard. It has become a key method of legal correspondence between governments, citizens, and businesses. The use of Certified Mail to send such important documents demonstrates the trust that postal customers place in it, leading some customers to use Certified Mail even when they are not legally required to do so.

Second, Certified Mail validates content. Parties in legal proceedings, especially in those where an individual is in conflict with a much more powerful entity, need to prove the validity of their evidence. For decades, Certified Mail has been a trusted method used by inventors, whistleblowers, advocates, artists, and others to prove that a document existed without alteration since the date claimed. For example, inventors will send designs to themselves via Certified Mail in case their creation or ownership is challenged. Whistleblowers will send vital documents to themselves via Certified Mail in case all other copies are destroyed. Or advocates will send contentious notes to themselves via Certified Mail in case their accuracy is questioned. If an envelope sent via Certified Mail remains sealed, the court accepts that the documents within have existed and remain unaltered since the day they were sent via Certified Mail. The use of Certified Mail to validate the authenticity of such important documents demonstrates the need for community validation of authenticity, leading many individuals in legally sensitive professions to rely upon Certified Mail as a best practice for data protection.

Unfortunately, there are many flaws in the current system:

1. Long Processing Times
   - A common complaint is the long processing time that occurs when an individual tries to send Certified Mail. There are several unique aspects of processing Certified Mail that increases wait times. First, individuals must wait in line to send Certified Mail if they want the postmarked receipt necessary for legal reasons. Second, it takes clerks longer to process Certified Mail transactions than many others.Third, the actual delivery of the Certified Mail can take 3 to 10 business days. And if the recipient is not available to sign at time of delivery, that timeline can increase to 15 days at which point the mail is returned to the sender of no signature is received.
2. Complicated Forms
   - For the average postal customer, properly filling out and attaching Certified Mail forms can be daunting. The process can be further complicated by adding a Return Receipt, which contains more fields to fill out. When an individual incorrectly fills out a form – a frequent occurrence – this results in the clerk personally having to assist the customer, extending processing times and frustration.
3. Delivery Reliability
   - Missing scans, signatures, and mail pieces present an acute problem in the case of Certified Mail. When a piece goes missing, no signature is obtained, or there is no final delivery scan, the sender is entitled to a refund from the post office

Aside from the financial risk posed by some of these delivery issues, delivery reliability is particularly important because much of Certified Mail's value comes from the ability to prove that delivery of the mail occurred. ***65 percent of Certified Mail users list confirmation of delivery as the main reason they use Certified Mail.***

4. Domestic Limitations
    - Certified Mail is a domestic mail product meaning the use of Certified Mail is limited to addresses within the United States. For international documentation validation, Certified Mail is not acceptable service.

Just as Certified Mail was developed as a better way to meet the emerging needs of customers in the 1950s, the antiquated and inefficient use of the U.S. Postal Service has paved the way for a new alternative in today's digital age.

Achieving the community validation offered by Certified Mail for digital files currently requires users to first reproduce a digital file in physical form. Outside of this traditional, antiquated documentation validation process, services such as Dropbox, Google Drive, other Cloud Storage providers, and dedicated data rooms strive to offer validation by providing auditable digital documentation protection. However, few digital documents in the legal community retain a fully autidable chain of custody within any of these systems. Without an external, community validation method for digital documents, when a digital document's validity is questioned during an eDiscovery process, the only way to currently attempt to resolve any validity challenge is through a forensic analysis which can easily cost in the range of $5,000 up to $20,000.

As the legal system begins to grapple with a world that has progressed from simple fraud to deep fakes, ***the truth provided by Certified Mail in the physical world needs a digital equivalent.***

Block 3: The Solution

Within the legal system, an industry where collaboration is key, trust is one of the biggest costs of doing business. The principle of trust is what led to the creation of blockchain technology.

Blockchain, for the majority of the world, is synonymous with Bitcoin, the peer-to-peer cryptocurrency introduced in 2009 utilizing blockchain technology to disrupt the banking industry. A blockchain essentially is a database or record-keeping technology that, instead of being held or recorded by one centralized participant, is shared across a network of participants. The name blockchain comes from the fact that information is stored in a chain of "blocks" of information. These blocks can store any type of information (in Bitcoin's case the information stored are centered around financial transactions including the date, time, amount, and participants). Once a new block is created, that information is needed to be added to the blockchain but first needs to be verified by all of the participants within the network, commonly referred to as "nodes". Once that block has been verified by the network, it is given what is called a "hash". This hash is a unique, identifying code that connects the blocks together in a specific order and allows anyone with access to the blockchain data to review any block with the identifying hash code. Once hashed, the block can finally be added to the blockchain and the process begins again for the next block of information.

With centralized control of a network, there is a reliance on a single authority whose job it is to organize the transfer of information. Therefore, trust plays such a large role. This centralized system has one major issue in that there is a single point of failure. The trusted authority may prove to be untrustworthy, eliminating all trust in the past, present, and future validity of the information stored within the network. However, blockchains present an opportunity to mitigate the single point of failure problem. With no trusted intermediary, information stored on a blockchain is maintained by the whole network, ensuring no single bad actor can exploit the network for their own benefit.

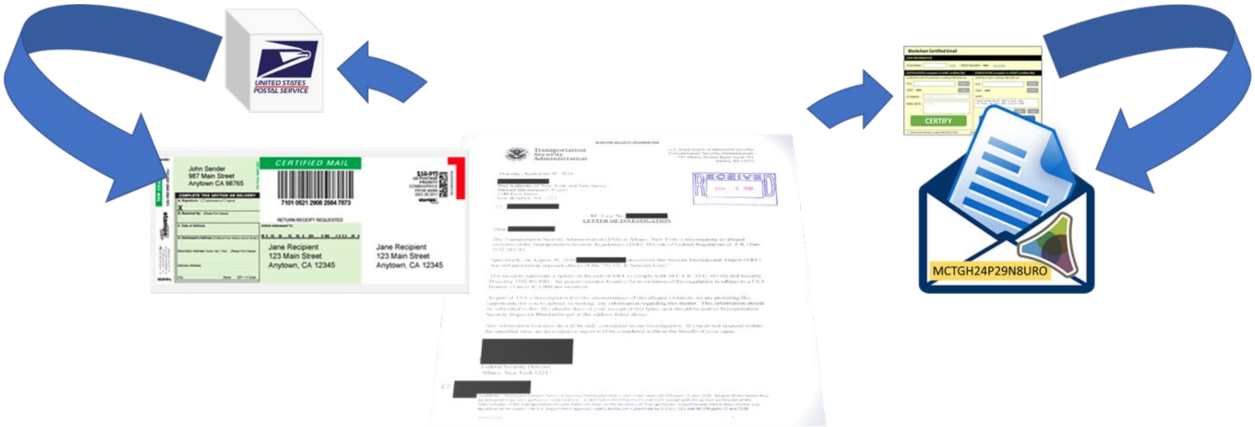
Trokt allows the legal community to own an immutable validation of its truths, regardless of their form or context. As previously stated, current blockchain solutions are not adequately solving this unique situation facing the legal industry. Enter the Trokt Blockchain. The Trokt blockchain ensures user access and preserves data distribution offering APIs that accept hashes of any data type (e.g. Word document, scanned image, email file) and encode only the hash and its timestamp. The defining and storing of any contextual data about a user who provides a data hash is dictated by the portal used to access a particular node.

Benefits of Trokt Blockchain for Democratizing Digital Truth

1. Efficient Processing
   - Compared to Certified Mail, the automated processing and elimination of complicated forms make for an efficient and painless exercise. Documents can be validated in minutes with the data hash and hash location shared with participants; the user experience simplified for ease of use for anyone.
2. Reliability
   - With the automated verification through the use of blockchain, document verification no longer relies on human error resulting in non-verification.
3. Low-Cost
   - Depending on the size of the document, the verification costs as low as $1 for a document 1MB or less (with the cost increasing $0.10 per each additional MB) whereas Certified Mail costs at a minimum $4.80.
4. Immutability
   - Once data has been written to the blockchain, no one has the authority to change it. Every member of the network independently checks and agrees that the integrity of the ledger is correct. Any changes that a party attempts to make to the blockchain are recognized and rejected by the majority of the network.
5. Transparency
   - Everything that takes place on the ledger is visible to anyone at all times. To that extent, if any documentation is ever recorded on the blockchain, anyone with access to the ledger will have access to that documentation to provide verification.

6. Irreversibility
   - Due to the immutability of the blockchain, anything entered onto the ledger is irreversible. Once verification of any documentation occurs, bad actors will be unable to reverse or remove the verification in any way.
7. Borderless
   - Compared to the limitations of Certified Mail, documentation verification through the Trokt Blockchain is not solely subject to the United States. Any individual with access to the network has the ability to utilize the network.

The Trokt blockchain is made up of 13 full nodes that archive data hashes, with each node accessed through any number of data submission portals. The default portal available to all nodes is the "Blockchain Certified Email" portal. The Blockchain Certified Email portal replicates the Certified Email system as follows:



1. A user selects a file to archive in Trokt,
2. User uploads the file via the Blockchain Certified Email form to be hashed,
3. The size and cost of archiving is computed and accepted by the user,
4. The hash is written to Trokt,
5. The data hash and hash location are written into an email to which the original file is attached,
6. The data hash and hash location are written into a Trokt document and, if elected, the uploaded file is stored in the Trokt document,
7. The email is sent and Trokt document shared with the owner of any email address specified by the user; and
8. Any user may verify that a file is in the Trokt blockchain by uploading the file for Trokt to hash, check against all ledgers, and return any location where that hash is archived by Trokt.

The base Blockchain Certified Email portal will save user email, IP address, and a pointer to the blockchain location. Additional node portals may require and store significantly more data about a user of any particular portal.

The basic Blockchain Certified Email portal is designed to be simple for anyone to use, powerful in its ability to validate any file type, and democratized in its opportunity for the legal community to own the immutable record that any citizen can use to protect themselves.

Block 4: Governance

Trokt will manage communication within the Trokt blockchain network of 13 full nodes. Governance, commercialization, and revenue distribution for each node will be controlled by the individuals or organizations who collectively own the transferable license for that node. All full node license owners must both (i) own at least 1% of the Waves generated Trokt token for that node and (ii) pay their portion of the annual license fee. The owners of a node will set the rules for what portals may connect and write to their node, with Trokt able to veto the connection of any node that would diminish the value of the overall network. The node owners may charge any portal provider any cost for any function that is mutually agreed to by the portal provider and node owners so long as that price per function does not diminish the value of the overall network. Each node license owner must pay every other node license owner a $0.02 operations fee per hash written. These operations fees per hash written will be divided among the owners of the node license as per the governance rules of that node.

Revenue Model Example: Blockchain Certified Email

Every full node will be automatically connected to a Blockchain Certified Email portal. Users may store the hash of any document to Trokt by using a nodes Blockchain Certified Email portal in exchange for 10 credits for the first megabyte of file size plus 1 credit for every additional megabyte, with each credit costing $0.10. To write the hash of a 0.8MB file to Trokt will produce $1.00 of revenue for the full node license holders.

Of this $1.00 in revenue, $0.02 must be sent to every other node license ownership team. Therefore, writing the hash of this 0.8MB file to its node will net the node license ownership team $0.76, and it will net all other node license ownership teams $0.02.

Annual License Pricing

Any individual or organization that owns at least 1% of the Trokt token for a node may bid to purchase up to three years of node licenses. The Fiscal Year 2020 guide price for a full node license is $50,000 per year. The winner of the node license auction may sell any portion of the license to any organization or individual who owns at least 1% of the Trokt token for that node. It is the responsibility of the node license owner to sell any portion of the node license in accordance with all appropriate laws and regulations.

If a qualified buyer wishes to purchase a full node outside of the auction period, he or she would be able to force the current license owners to match a bid that is at least 150% the value of the current license price. If the current owners do not wish to match the increased license value, the qualified buyer would buy out the current license contract for 1.25x the remaining value of the license price. In an instance of a forced purchase, a new Trokt token would be issued and awarded to the buyer for resell.

Trokt Node Tokens

Trokt will issue one Waves-based token with five decimal places for each full node. These tokens may be bought and sold with no restrictions and provide the owner the right to purchase in whole or a portion of a full node license if he or she acquires at least 1% of the token created for each node. If the owners of at least 30% of a Trokt token are confirmed to be inactive or unreachable, Trokt will reissue a token for a node if requested by 90% of all active token holders. When reissued, all active token holders will receive a percentage of the issuance proportional to their position within the group of active token holders.

Individuals who are not comfortable creating and managing a cryptocurrency wallet may contract with Armetis Ventures to provide wallet management services for an annual retainer plus direct transaction costs.

Full Node Operations

The operation of each node, to include hosting, will be managed by Trokt unless a node owner identifies an alternative that does not compromise the quality or value of the network.

Block 5: The Team

The Trokt blockchain leadership team is built around 3 team members whose combined expertise cover legal security, data protection, and blockchain markets.

Chris Draper, Ph.D., P.E., Managing Director

Chris is an expert in the operation of human-technology interfaces, specializing in how individuals use technology to collaboratively manage legally sensitive data. He is a regular speaker, author, and instructor on issues of operational security, digital data risk, and technology ethics. Chris received a Bachelor of Science degree in Mechanical Engineering from the University of California at Berkeley and a Doctor of Philosophy degree from the University of Glasgow.

Joe Vande Kieft, Technology Director

Joe is a seasoned CTO and technologist specializing in database construction and legally sensitive communication systems. His architecture and development background include email and text messaging systems that are depended on by Federal and state governments. Joe received a Bachelor of Arts degree in Computer Science from Central College.

Corey Pigott, Blockchain Advisor

Corey is a Venture Partner at the San Francisco-based family firm DraperFoster specializing in blockchain and cryptocurrency technologies and markets. Corey is the Founder of Armetis

Ventures, a boutique asset management firm focused on investing and actively managing a portfolio of cryptocurrencies and digital assets for a small group of high-net worth investors, which he launched after nearly a decade at Crypto.IQ and Interactive Financial Advisors. Corey received a Bachelor of Arts degree in Finance from California Polytechnic State University at San Luis Obispo.

Block 6: Conclusion

Trokt is proposing the evolution in truth validation that will finally incorporate a constantly maturing digital world. The framework for how the legal industry protects its data is always improving. In the same light, the framework surrounding data validation will also require improvements to stay relevant in the digital age. Improvements to many current issues including reliability, accessibility, transparency, and efficiency will do wonders to minimize the cost, errors, and time associated with distributed truths and the potentially tedious process of challenging validations of these distributed truths. At scale, it will no longer be sufficient for our modern legal system to simply address the storage and management of distributed truths.

The secure validation of community truths will be the defining cornerstone of the current LegalTech revolution.