Use Cases for Trusted Workflows

Practical Applications for Proof Systems

14 September 2016
Paradigm Shift

We see the world positioned at the beginning of a massive paradigm shift in information technology.

This shift is coming from dramatic increase in connectivity thanks to widespread internet access and devices, the development of modern cryptography, and decentralized peer-to-peer systems.

A hundred years ago, information was stored in cards, in boxes, and locked in a room. The keyholder to this room held control over the access to this information, and thus the power of the information. Today, our information systems have been built in this old paradigm, and we have inherited the recurring issues of this aging paradigm:

1. **Security Risks Due to A Single Keyholder**
   If there is a single keyholder, then the security of that information is only as strong as the security of the keyholder.

2. **Synchronization Complexity Due to Isolated Silos of Information**
   Synchronizing siloed systems demands intensive manual labor and both digital and paper audits from trusted third parties.

3. **Reduced Individual Control over Private Data**
   Individuals are asked repeatedly to share their own private information with many institutions, and thus must trust in the institution’s single keyholder security.
New Solutions

Stratumn is dedicated to solving these issues by leveraging the latest advances in cryptography, peer to peer systems, and blockchains to offer a platform for trusted workflows.

Trusted Workflows are organizational processes powered by applications that provide a transparent, provable, and immutable audit trail of digitally notarized data, effectively addressing each of the three recurring issues from the old boxes-in-a-room paradigm.

Security risks associated with a single key holder are addressed by issuing many keys to various actors of a network. While it is possible to compromise one key, compromising an entire network becomes impossible.

Synchronization is addressed through blockchains through the elegant implementation of a consensus model. Notably, by utilizing a consensus model, Bitcoin was able to solve the critical issue of double spending, which had stopped the success of many previous digital currencies.

Individuals are able to take back control over their own data with the ability to share cryptographic proofs of its validity, allowing businesses and regulatory authorities to fulfill their roles with less overhead and less risk to individuals by storing their information.

Thanks to the development of bitcoin and other blockchain networks, we can now begin to build systems that expand upon the use case of a digital currency. This document describes in detail the unique ways that several of these use cases could work.
New Possibilities

Stratumn offers a set of services to complement blockchains that offers several key new benefits for enterprise.

With this infrastructure in addition to a blockchain, your organization can begin to embrace the unique benefits and power of trusted workflows.

**Digital Notarization**
Digital files can be signed through a process of cryptographic hashing and timestamping, creating an immutable blockchain record with a unique digital signature.

**Universal Traceability**
The origin of any document, contract, or piece of media can be traced independently of any single actor or system by using publicly available tools.

**Digital Ownership**
Digital assets that represent real world properties such as documents, source code or physical objects can be issued and transferred, and capture a precise record of any modifications to the property.

**Proof of Process Reporting**
At any point a report can be generated that visualizes and describes in detail dates, times, metadata, and signed cryptographic proofs of any part of a workflow.

**Direct Settlements**
Any type of good, product, or information can be securely exchanged in accord with the logic of a smart contract, without the involvement of intermediaries.
Use Case #1

Know Your Customer (KYC)
Standard KYC

The Problem

In a time in which people quickly change their jobs, locations, and business services, KYC processes have become a mandatory part of many banks, insurers, and other businesses’ operations.

The current standard process satisfies functional requirements for the business and regulatory authorities, but becomes increasingly costly and complex as technology and regulations evolve.
For each new business service, the customer must go through this process again, often with slightly differing requirements that demand significant back and forth communication between parties.
The standard KYC process is highly redundant and inefficient, resulting in significant friction points.

**Poor Customer Experience**
Customers must submit the same documentation multiple times, often with slightly different requirements, with each new registration process.

**High Operational Cost**
Institutions must invest in significant man-hours to gather relevant documents and auditing for compliance. In the field of retail banking, 37 days is the average amount of time for corporations and 12 days for private individuals.

**Inflexible Technology**
Siloed systems often cannot efficiently adapt to the demands of changing regulatory requirements.
Trusted Workflow KYC

The Solution

Trusted Workflows allow for the implementation of a KYC process that allows participants to efficiently use existing relationships and essential data to create a secure “trust network” without revealing sensitive data. The trust network in turn reduces operational costs and allows for a smoother and faster customer experience.
Acquisition of Personal Information
Private documents are selectively shared by a customer with a trusted regulator, government entity, or licensed partner.

Validation of Personal Information
The trusted party reviews and verifies the authenticity of the documents, then produces a digital signature from the documents’ cryptographic proofs, which is then notarized onto a public blockchain.

KYC Token Issuance
A cryptographic token is generated for the customer, which can be used to verify the authenticity of the trusted party’s signature, the documents, and thus the validity of each step of the KYC process.

Ongoing Updates
As some documents become obsolete or invalid, a workflow is introduced and updates are timestamped into a public blockchain to prove the validation of these documents by a trusted party.
Trusted Workflow KYC
Process

1 **Token Presentation**
Because the customer already has his documentation validated, he can present the token as cryptographic proof.

2 **Token Validation**
With the token and signed hashes in the blockchain, the service business can use independent techniques to verify its validity.

3 **Token Update**
Once the new service has validated the customer’s token, the service can sign the confirmation of the customer’s validation into a blockchain, giving the customer an updated token which includes the additional record of validation.
Improved Customer Experience
When a customer begins a registration process with a service company, he can share an identity token instead of the original documents.

Cost Reduction
By reducing the redundancy in the verification process and automating reporting, Blockchain KYC can reduce costs for all participating parties.

Improved Compliance
The proofs of all steps of Blockchain KYC can easily (and automatically) be shared with regulators.
Trusted Workflow KYC with Stratumn and Chainscript offers several unique features that benefit both businesses, regulators, and customers.

**Digital Notarization**
Digital files can be signed through a process of cryptographic hashing and timestamping, creating an immutable blockchain record with a unique digital signature.

**Universal Traceability**
The origin of any document, contract, or piece of media can be traced independently of any single actor or system by using publicly available tools.

**Proof of Process Reporting**
At any point a report can be generated that visualizes and describes in detail dates, times, metadata, and signed cryptographic proofs of any part of a workflow.
Use Case #2

Shipping
Shipping goods is a dynamic problem that demands continual consensus from a variety of parties that may be spread throughout different parts of the world and who may be using completely different information tracking systems. This situation leads to significant challenges for all parties involved in the shipping process.
The standard method of shipping is made difficult due to the challenges of sharing information between systems, unsynchronized payments and deliveries, and auditing.

**Tracking Goods Between Different Delivery Partners**
Several delivery partners may be involved during the process of moving and storing goods. Each partner may have their own siloed digital or paper information system.

**Unsynchronized Payments and Deliveries**
Synchronizing payment and delivery is difficult as payment is either pre or post trade, leading to increased friction during the customer journey.

**Paper Document Auditing**
Regulators and stakeholders may need to audit the entire supply chain process, but data may be corrupted or difficult to access.
Trusted Workflow Shipping

The Solution

By implementing blockchain notarization, shipping partners can increase both the interoperability between all parties as well as the security of the data, leading to reductions in cost and improved traceability and compliance.
1. **Shipping Service Loads a Container & Signs Its Receipt**
   When the container is ready, its identifying information and its cargo are hashed and timestamped (digitally notarized) in a blockchain.

2. **Customs Reviews the Cryptographic Certificate’s Validity**
   Regulatory authorities query the blockchain to view the digital proofs of the supply chain process.

3. **Container is Shipped and Unloaded to a Freight Train**
   Operators sign this step with their unique keys, notarizing this fact in the blockchain.

4. **Warehouse Receives the Container**
   Once it arrives at its final destination, the container is unloaded and the receiver accounts for the cargo and individually notarizes each item received with a digital tag.
Trusted Workflow Shipping

Benefits

Systems running Trusted Workflows synchronize data from multiple parties while generating an audit trail that can be used to ensure data integrity and regulatory compliance.

Standardized Tracking
A real-time audit trail can be generated during the shipping and storage of goods with timestamps and digital signatures for each step with every partner.

Payment and Delivery Synchronization
Payment can be automatically released once a customer digitally signs a receipt of delivery and the transaction has been notarized on the blockchain.

Compliance & Data Integrity
Documents and receipts of the process are automatically tied to a cryptographic audit trail which can be used to prove the validity and integrity of the data. Any stakeholder or regulator can validate this data through its unique identifier in the blockchain.
Universal Traceability
The origin of any document, contract, or piece of media can traced independently of any single actor or system by using publicly available tools.

Direct Settlements
Any type of good, product, or information can be securely exchanged in accord with the logic of a smart contract, without the involvement of intermediaries.

Proof of Process Reporting
At any point a report can be generated that visualizes and describes in detail dates, times, metadata, and signed cryptographic proofs of any part of a workflow.

The benefits of Trusted Workflow Shipping with Stratumn and Chainscript can be realized through these new possibilities.
Use Case #3

Microinsurance
Trusted Workflow
Microinsurance

Concept

The sharing economy has disrupted a variety of industries and increasingly the very idea of ownership is becoming more fluid among younger people, thanks to the spread of the internet and various sharing platforms.

By integrating with social platforms and notarizing transactions on a public blockchain, insurance companies can provide a better user experience that is suited to the age of the sharing economy.
Trusted Workflow Microinsurance Process

1. Lending Agreement Proposal
   A lender can propose to lend a piece of his personal property that he has digitally registered through his insurance provider (through the unique product SKU) to another user through an insurance Chatbot on a public platform such as Facebook or iMessage.

2. Agreement Review
   The borrower reviews the proposal from the lender through a message received from the insurance Chatbot, and can accept or decline the proposal.
   If he accepts he can go through an onboarding process and purchase the insurance through a payment processor.

3. Agreement Signature and Notarization
   Once the borrower agrees to the proposal and confirms that he has received the piece of property, the agreement is digitally signed and notarized onto a public blockchain, creating an immutable cryptographic audit trail of the agreement.

4. Confirmation Token Issuance
   Both the lender and borrower receive digital tokens that can be issued to cryptographically confirm that both parties have signed the agreement.
**Trusted Workflow Microinsurance**

**Benefits**

**Trusted Workflow** offer dramatically increased flexibility and new methods of customer engagement.

**Improved Customer Engagement**
Seamless coordination between systems allows insurance companies to more efficiently onboard new customers and more quickly respond to customer’s requests.

**Cost Reduction**
Because there is an immutable audit trail for every agreement, verifying the validity of insurance claims becomes significantly easier.

**Reputation**
By helping customers to share items with friends, family, and colleagues, both the customers and the insurer can develop a positive reputation that can be publicly verified without disclosing details about specific agreements.
Truste d Workflow Microinsurance
New Possibilities

The benefits of Trusted Workflow Microinsurance are unique facets of these new possibilities.

Digital Notarization
Digital files can be signed through a process of cryptographic hashing and timestamping, creating an immutable blockchain record with a unique digital signature.

Digital Ownership
Digital assets that represent real world properties such as documents, source code or physical objects can be issued and transferred, and capture a precise record of any modifications to the property.

Proof of Process Reporting
At any point a report can be generated that visualizes and describes in detail dates, times, metadata, and signed cryptographic proofs of any part of a workflow.
Use Case #4

Clinical Trials
Clinical research is undergoing a crisis of both irreproducibility and hyped up results. The standard procedure for clinical trials today being vulnerable to poor design, opaque methods or data corruption, masked behind a clear lack of transparency.

This crisis has been fostered by conflict of interests, pressure to publish in quantity rather than quality, and to yield positive results to access prestigious journals (“Publish or Perish”). However, step by step, scientific processes can be improved to get closer to its ideal form.
Standard Clinical Trial Process

1. **Trial Design**
   The trial must be clearly defined with primary and secondary endpoints, as well as methods of recording and keeping statistics.

2. **Patient Enrollment**
   Patients must give informed and free consent to participate in the trial.

3. **Clinical Data Collection**
   Data is collected through various means and often recorded through double entry.

4. **Data Analysis**
   Data must be analyzed in accordance with the methods defined in the trial protocol.
Lack of transparency is a major obstacle to a good scientific process

Corruption of the results
Study design, methods and objectives are not always shared prior to a study, allowing modifications to favor the outcome of a favorable trial result. The same applies for the sharing of the data (raw data is often inaccessible), opening a breach for data corruption.

Opacity of study
Because the information shared are partial and the study sometimes poorly designed, it makes it difficult, if not impossible for those who may want to reanalyze or replicate the findings.
Trusted Workflow
Clinical Trials

The Solution

Leveraging a design based on a cryptographic audit trail, this solution encourages stronger study design and discourages non-legitimate alterations of the study or its data, building more integrity and transparency into the research process.
1. **Digital Notarization of Study Design**
   The original design and methodology of the trial and its objectives are recorded and notarized in the blockchain.

2. **Patient Consent Notarization**
   The investigator must obtain free and informed consent from the patient.

3. **Fulfillment and Notarization of Surveys**
   Patients fill out surveys which are signed and cryptographically notarized into the blockchain, providing a timestamped recorded of the collection of all results.
   Raw survey data is securely stored in a research center database.

4. **Clinical Trial Audit**
   With the access to the proofs of the existence of the information, regulators and other researchers can verify the integrity and authenticity of the data and study.
Trusted Workflow Clinical Trials offer the potential for stronger data integrity and improved trial reproducability.

**Prevention of corruption**
Proofs of initial protocol design and methods ahead of the study, as well as chronological proofs of the progress and data collected are stored, enabling to easily audit information and determine if there has been any corruption. As it is proofs of the information and not the data itself that is notarized, confidentiality and security are never compromised.

**Trial Transparency**
With no more incentives to hide or alter the protocol and the data collected, incentives to share details with the rest of the research community improves, facilitating the replication of the study.
Digital Notarization
Digital files can be signed through a process of cryptographic hashing and timestamping, creating an immutable blockchain record with a unique digital signature.

Universal Traceability
The process through which any document, contract, or piece of media follow and interact with each other can be traced independently of any single actor or system by using publicly available tools.

Proof of Process Reporting
At any point a report can be generated that visualizes and describes in detail dates, times, metadata, and signed cryptographic proofs of any part of a workflow.