The MediLedger Project 2017 Progress Report

February 2018
by:

CHRONICLED

Genentech
A Member of the Roche Group

McKESSON

AmerisourceBergen®

Pfizer

abbvie

Table of Contents

1 EXECUTIVE SUMMARY

The **MediLedger Project,** established in 2017, brought together some of the world's leading Pharmaceutical Manufacturers and Wholesale Distributors to explore the potential of blockchain technology in the track and trace of prescription medicines. Our scope was to evaluate the feasibility of a blockchain based solution for compliance with The Drug Supply Chain Security Act (DSCSA) with the understanding that the conclusions can be extrapolated to other potential use cases.

Based on business requirements and guidance from our working group, the MediLedger Project developed a blockchain-based system for tracking the legal change of ownership for prescription medicines. In summary, The MediLedger Project has drawn the following conclusions so far:

- Blockchain has the capability to be the interoperable system for the pharmaceutical supply chain, as mandated by DSCSA. Transaction throughput, speed, and reasonable cost can be achieved to meet stakeholder needs.
- Data privacy requirements of the Pharma industry can be met using "*zero knowledge proof"* technology, where all transactions posted to the blockchain are fully encrypted - ensuring no confidential information is shared. The design allows for nodes in the blockchain system to be hosted by a number of unique parties while maintaining strict transactional privacy and ensuring immutability of the transactions.
- A blockchain system can be capable of validating the authenticity of product identifiers (verification) as well as the provenance of sellable units back to the originating manufacturer.
- The authenticity of the drug can be confirmed with each transaction allowing for expedited suspect investigations and recalls.
- The Working Group believes that should a blockchain ecosystem be created as a possible solution to the DSCSA interoperable solution requirement, it should have an open system architecture with an appropriate governance to oversee the function of the system and ensure compliance with industry agreed business rules and standards of operation.
- The trust established by a blockchain system can be leveraged for a myriad of additional business applications to the pharmaceutical industry, allowing for compounding benefit for this industry once such a platform is established.
- The long-term success of a truly interoperable blockchain-based solution will require strong participation from all industry stakeholders (manufacturers, wholesalers, dispensers, service providers, etc.).

The work to date has indicated that a blockchain-based system appears to meet the system requirements set forth by DSCSA for an interoperable system. To note: participants in a blockchain-based system will be responsible for determining and ensuring their own compliance with the DSCSA and other applicable laws.
The Working Group will continue to evaluate this further for pharmaceutical track and trace solutions.

2 2017 WORKING GROUP APPROACH

The Working Group was established in 2017 to bring together representatives from leading pharmaceutical manufacturers, wholesale distributors, supply chain management experts and various companies to determine what blockchain could potentially provide in terms of improved solutions for the pharmaceutical industry. Its goals for 2017 were the following:

- Model events in a serialization data exchange environment for prescription drugs using a blockchain-distributed ledger system.
- Determine a business and financial model that allows for the participation of the different industry stakeholders.
- Identify potential issues with system performance and capabilities.
- Define the potential IT architecture of an electronic interoperable system.
- Provide possible “path forward” recommendations to the industry.
- Share blockchain knowledge, separating reality from the hype.
- Demonstrate how blockchain technology may be better suited than others to respond to DSCSA requirements and how it can provide other strategic advantages.

The Working Group’s guiding principles were:

1. PATIENT SAFETY: Improve drug supply chain security and protect the patient
2. INDUSTRY FIRST: Industry benefits as a whole are important and are the constant focus of the working group
3. SIMPLICITY: The system must be simple and easy to adopt by most stakeholders

A technical prototype to demonstrate that blockchain could meet both the requirements of the DSCSA regulation as well as the operational expectations of the industry was built. Once this prototype was ready, the Working Group focused on how such a system could be set up, governed and operated to benefit patients and help facilitate compliance with DSCSA.

This Working Group also defined a set of requirements that the system must meet:

2.1 System Requirements

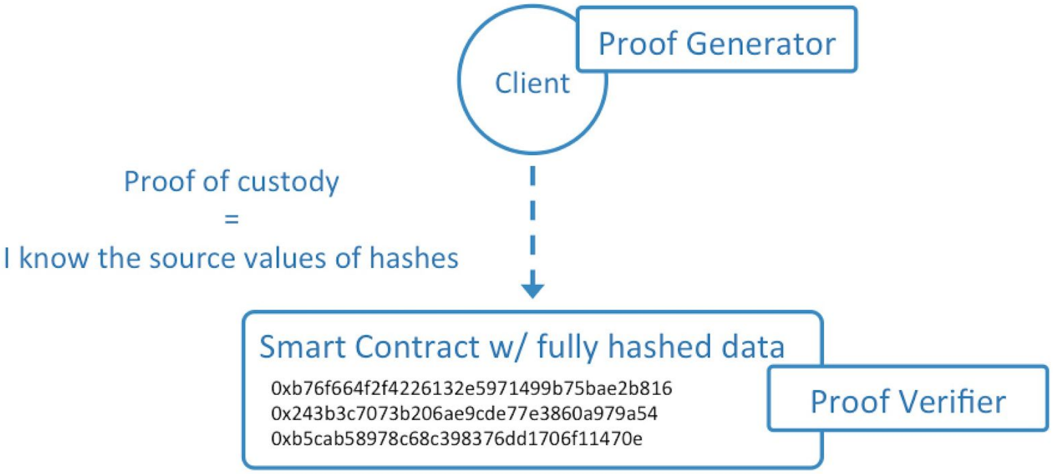
- Enables any interested organization in the industry to plug into the system
- Ensures privacy of data committed to the blockchain ledger with zero leakage of business intelligence
- Able to process 2000+ transactions/second (industry estimate)
- Can complete verification requests in less than 1 second
- Can solve aggregation/de-aggregation, saleable returns and exception handling scenarios
- Can create a level playing field to eliminate potential for vendor lock-in

2.2 Prototype Solution

The MediLedger prototype system was built on a Parity Ethereum client. Through the demonstration of functionality, the prototype met all of the above system requirements.

3 TECHNOLOGY SOLUTION

The MediLedger prototype solution uses a permissioned ledger and employs *zero-knowledge proofs* to allow fully hashed data on the blockchain, while still enabling the smart contract to enforce critical business rules (e.g., a serialized unit cannot exist twice in the system at any one time). In cryptography, a *zero-knowledge proof* is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.


Proof Generator
Client
Proof of custody
=
I know the source values of hashes
Smart Contract w/ fully hashed data
0xb76f664f2f4226132e5971499b75bae2b816
0x243b3c7073b206ae9cde77e3860a979a54
0xb5cab58978c68c398376dd1706f11470e
Proof Verifier

The solution is based on zk-SNARKs and leverages the work done by researchers at University California-Berkeley and MIT to make Non-interactive Zero-Knowledge Proof practical and applicable to business rules.[1]

[1] While a lot of research papers were published from the inception in 1992 [Joe Killian, link], today's practical implementation of zk-SNARKs is best represented by "SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge" [link] "and Quadratic Span Programs and Succinct NIZKs without PCPs" [link].

3.1 System Architecture

The key technical components of the MediLedger architecture are:

A private **Client** is an application process interface that is unique to each participant and hosts private data. It performs the following functions:

- Receives transaction data
- Exchanges messages with authorized trading partners' Client applications
- Securely stores private data, including transaction data
- Prepares transactions to be posted to the blockchain by calculating hashes and mathematical proofs
- Posts transactions to a Node of the blockchain and verifies that they are successfully accepted

A blockchain **Node** is tasked to maintain the blockchain security by participating in the consensus process of validating a proof of work. A Node delivers the following:

- Validates transactions
- Secures blockchain via consensus
- Provides the zk-SNARKs support in conjunction with the **Client** software
- Hosts the Smart Contract, which implements the core business logic and verifies the mathematical proofs

The system architecture for the prototype was designed to establish a secure blockchain network and reduce overall costs while processing over 2,000 transactions per second.

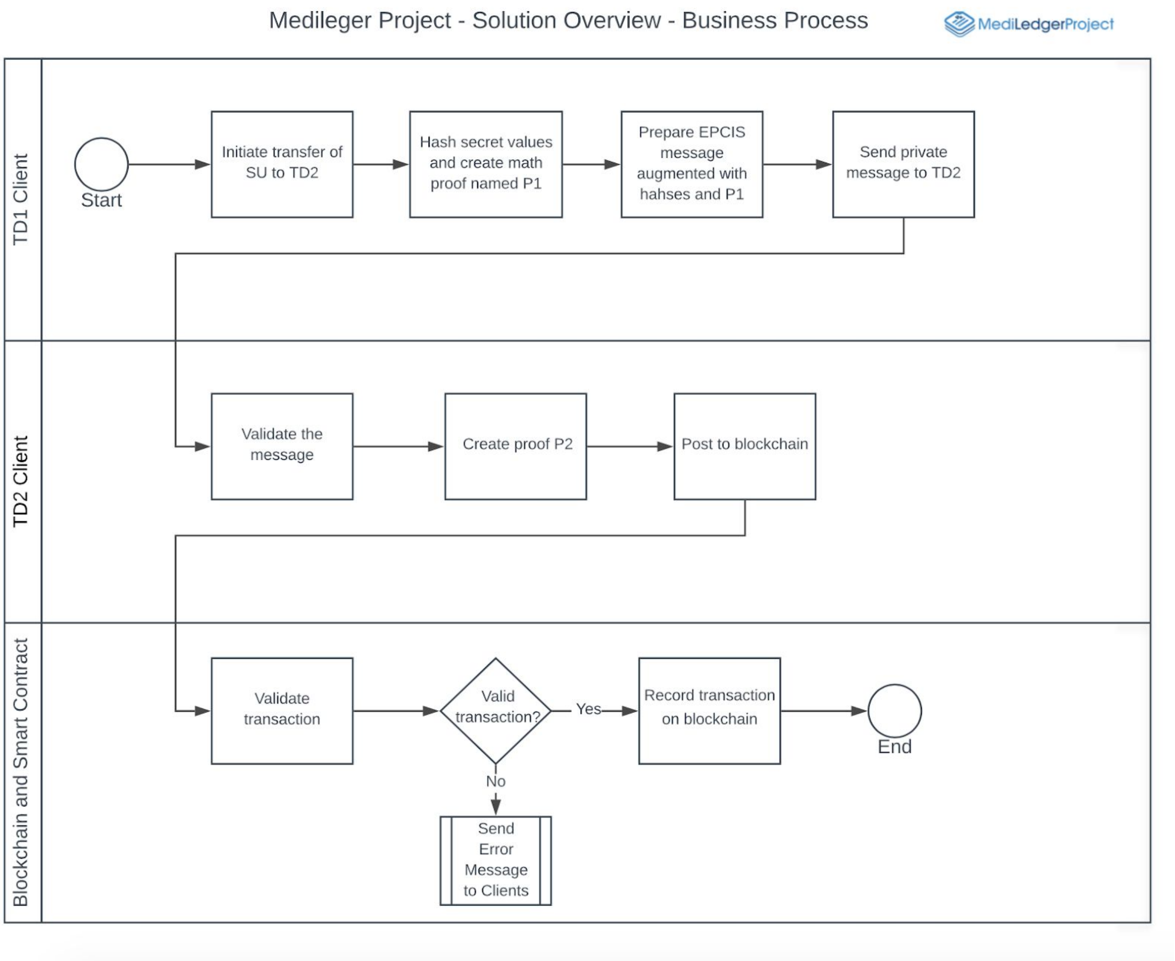
3.2 Solution Overview

In order to prevent the double transfer of a serialized unit while ensuring transaction privacy, the solution uses three core technologies:

1. Private messaging between Clients to exchange confidential messages between trading partners by leveraging EPCIS technology and standards.
2. Blockchain as a shared, immutable ledger to register the proof of the authenticity of transactions and execute smart contracts. The blockchain will enforce business rules, such as only one company can have legal ownership of a serialized unit at a given time (no double transfer).
3. zk-SNARKs to further enhance privacy.

The key design pattern of the solution focuses on the handling of a serialized unit. Each unit is managed as a non-fungible token with the custody assigned to a trading partner. Custody of a serialized unit can be transferred and the transfer function is governed by the smart contract deployed on the blockchain. The current custodian initiates the transfer and the recipient of the transfer needs to accept it in order to complete the transaction.

The system will ensure that only the authorized manufacturer of a particular product can provision their own serialized units on the blockchain. Then a transfer of a serialized unit (SU) between a trading partner (TD1) and second trading partner (TD2) is described in this diagram (logic is included below):


Medileger Project - Solution Overview - Business Process
MediLedgerProject
TD1 Client
Start
Initiate transfer of SU to TD2
Hash secret values and create math proof named P1
Prepare EPCIS message augmented with hahses and P1
Send private message to TD2
TD2 Client
Validate the message
Create proof P2
Post to blockchain
Blockchain and Smart Contract
Validate transaction
Valid transaction?
Yes
No
Record transaction on blockchain
End
Send Error Message to Clients

- TD1 Client is instructed via an API call to initiate the transfer of SU to TD2.
- TD1 Client calculates its side of the blockchain transaction, which contains hashes of its secret values and a TD1 mathematical proof named P1.
- TD1 Client prepares an EPCIS message with proper instructions about the transfer (i.e., shipment in GS1 jargon).
- TD1 sends a private message to TD2 containing EPCIS data and the TD1 side of the blockchain transaction.
- TD2 formally validates TD1 message and prepares its side of the blockchain message that contains hashes of its secret values and TD2 mathematical proof named P2.
- TD2 posts the transaction to the blockchain.
- The smart contract validates the transaction by verifying both proofs P1 and P2. If valid, the smart contract updates its state by incorporating the hashes submitted in the transaction as part of the new state. These new hash values represent the transfer of custody of SU from TD1 to TD2.

Multiple variants of the solution were tested in order to confirm specific properties of the system.

3.3 Cleanroom Initiative

An independent review and validation of the MediLedger solution was performed by Alessandro Chiesa, faculty member in Computer Science at UC Berkeley (one of the inventors of zk-SNARKs), Zaki Manian, Executive Director at Trusted IoT Alliance, and David Schwartz, Chief Cryptographer at Ripple. They followed this process for their assessment:

1. Held a workshop to review the solutions
2. Produced a white paper
3. Held independent, offline reviews by each cryptographer
4. Created final statements

The 3-month review process was thorough and included the review of the MediLedger's technical white paper of the solution. The reviewers confirmed the efficacy and performance of the method against its intended purpose. The output of the cleanroom initiative was posted on reddit. Please see Appendix A for the individual and joint statements.

4 VISION FOR USE OF BLOCKCHAIN

The MediLedger Work Group believes that the establishment of a blockchain ecosystem for the Pharma supply chain may be a possible solution to the DSCSA's interoperable system requirement. With the right infrastructure and governance framework, such an ecosystem is viable and may be able to provide a potential solution for the entire Pharma industry.

4.1 Future Solution Structure

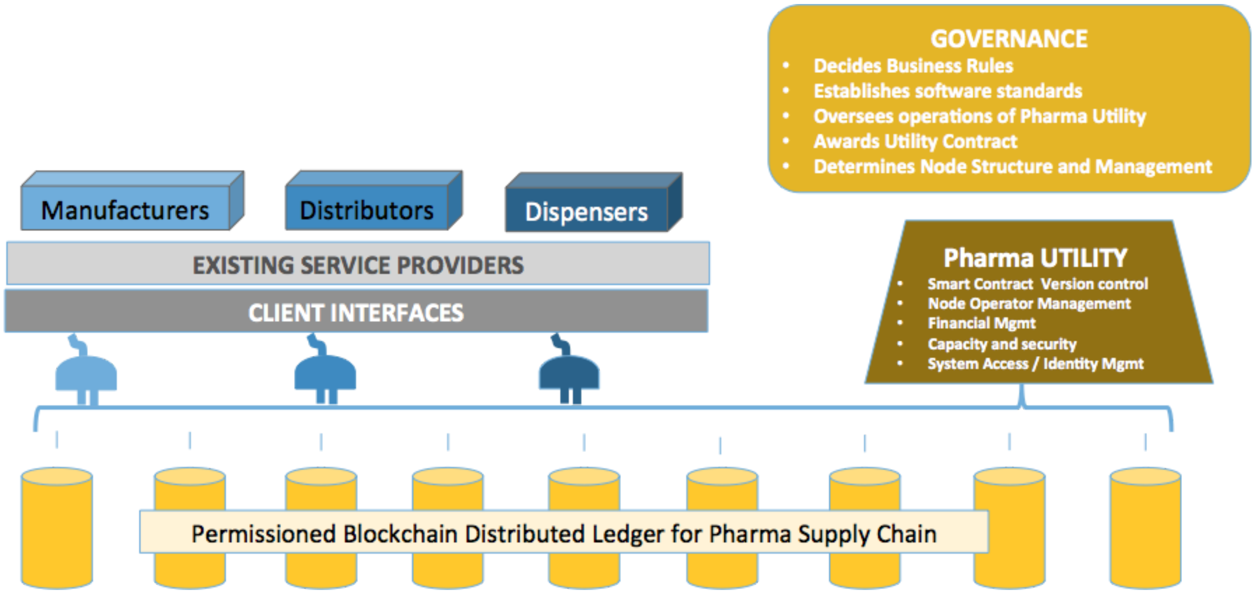
A blockchain ecosystem for the Pharma Supply Chain, if adopted, would consist of four main components:

- **Blockchain Nodes**: As described above, the nodes are the distributed ledgers where transaction/event information is replicated and stored. In practice, a customer of the system would choose a node to post their transactions, and then the blockchain software would automatically establish consensus among the nodes, and pass those transactions to the other nodes so that each holds the same record of events that happened. The node software will also ensure that records stays synchronized across the network, and will send alerts when it appears that the data is not correct. The nodes for the MediLedger network will be owned and operated by Pharma companies and accredited service and technology providers. This truly distributed network is possible through the zk-SNARKs data privacy solutions provided by the system and will allow for a truly immutable ledger.

- **Customer Client**: Clients are designed to easily communicate with other participating system members (for example trading partners, system solution providers, etc.). Clients will utilize EPCIS messaging to transmit EPCIS serial number data and proofs of the transactions will take place client to client. Clients will also allow members to do rapid verification of their serial numbers, as well as answer verification requests. With the system specifications open, this will allow for anyone to create and manage a client software using the MediLedger platform.

- **Utility**: The Utility will be tasked with maintaining the operations of the blockchain ecosystem under the oversight of the cross-industry Governance body (described below) and would have five main functions:
  1. System Access and Identity Management - would provision identity and access to participate in the system in line with the roles defined in the DSCSA (Manufacturer, Distributor, Dispenser, etc.).
  2. Node Operator Management - would determine who is allowed to operate nodes, and oversee certification and audit of node operations.
  3. Client Certification/Software Version Control - would determine compliance with open system architecture requirements and ensure all software updates are provisioned appropriately.
  4. Capacity Management - would ensure the system is set up to operate and scale appropriately as system usage grows.
  5. Financial Management - would perform monthly financial "true up" between nodes to pay for consensus support of node network, as well as financial operation of the Utility itself.

- **Governance**: For such an ecosystem to be effective, The Working Group believes that governance should be owned and operated by the industry, with standards and rules discussed, reviewed and approved by a governance body comprised of representatives across the pharmaceutical industry. This cross-industry governance body will be tasked to provide oversight to the ongoing growth and expansion of such an ecosystem and done to best serve the evolving needs of the pharmaceutical industry. Key responsibilities:
    1. Establishing the software standards to be used
    2. Deciding on business rules to be followed and enforced
    3. Oversight of the Utility
    4. Ongoing review and approval of smart contracts



GOVERNANCE
Decides Business Rules
Establishes software standards
Oversees operations of Pharma Utility
Awards Utility Contract
Determines Node Structure and Management
Manufacturers
Distributors
Dispensers
EXISTING SERVICE PROVIDERS
CLIENT INTERFACES
Pharma UTILITY
Smart Contract Version control
Node Operator Management
Financial Mgmt
Capacity and security
System Access / Identity Mgmt
Permissioned Blockchain Distributed Ledger for Pharma Supply Chain

4.2 Guidelines for Governance

Governance for a blockchain platform will be critical for such a system to operate effectively and gain adoption. The success of governance lies in performing only the necessary oversight of the system - what minimally needs to be done the same - thereby allowing for innovation and free market competition for the provision of services related to aspects of the platform.

Further work needs to be done to determine if existing infrastructure already exists that could be an appropriate “home” for such governance. Regardless of where this governance will finally sit, a key expectation is that it will be collaboratively performed with industry working groups and will leverage dialogue and decisions made elsewhere to be implemented on the blockchain.

5 CONCLUSIONS AND NEXT STEPS

The Working Group believes that a blockchain-based system can meet the requirements of an industry-level system that tracks changes in ownership of prescription medicine consistent with DSCSA requirements. It also agrees that the establishment of a system recording the change of ownership of prescription medicines can provide the opportunity to automate business processes associated with that transfer, but the possibilities to transform supply chain operations deserves further review.

The MediLedger Project's work will continue in 2018 with the following goals:

- Identify a framework for Pharma industry governance for blockchain-based track and trace solution
    - Develop potential structure of industry blockchain platform, including standards, functionality, business priorities
- Continue the evaluation of a possible blockchain ecosystem with the following objectives:
    - Key DSCSA and industry requirements are included in prototype design
    - Provide opportunity to test data/product ownership transfer and verification between members of the Working Group as appropriate
    - Provide opportunity to establish nodes and gain experience through node management
- Determine Service Provider Integration
    - Meeting with service providers to determine potential path forward for integration into a blockchain platform
    - Ability to design for multi-use business applications

Chronicled is grateful for the partnership and the collaboration of the 2017 MediLedger working group. We would like to say thank you for the leadership and valuable guidance of: **Genentech** - Nirmal Annamreddy, Kathy Daniusis, Krzysztof Jurkowski, Jaya Kala, Mark Mcloughlin, Pablo Medina, David Vershure; **AmerisourceBergen** - Jeffery Denton, Matt Sample, Heather Zenk; **McKesson** - Matt Langford, Scott Mooney; **Pfizer** - Byron Bond, Susan Graser, Mack MacKenzie, Michael J. Mazur, Andrew Schmitt; **Abbvie**: Julie Kuhn, Lloyd Mager, David Otterness, Mike Zupec.

We look forward to 2018 and are excited about the possibilities to establish a possible robust platform and process that enables companies to meet FDA regulations, improve their supply chain operations and reduce counterfeit drugs.

Appendix A: Clean Room Initiative

Individual statements

Alessandro Chiesa
Assistant Professor, University of California at Berkeley
The Chronicled pilot marries blockchain and zkSNARKs technology with an application to the supply chain industry. I was pleased with how Chronicled Blockchain Engineer Maksym Petkus was able to build on top of the libsnark codebase to deliver a custom implementation that fits exactly their intended purpose, which was to establish a secure and connected record of custody while maintaining full privacy and without the potential for double-transfers of the SGTINS between trade partners. After the initial review, we asked the Chronicled team to write-up a formal mathematical representation of the solution, which was completed to a very high standard of quality.

David Schwartz
Chief Cryptographer, Ripple Labs
I participated as a reviewer in the Chronicled cleanroom assessment of their zk-snark supply chain implementation. Our review process involved spending a 6 hour session at the Chronicled office, examining the codebase and implementation, and openly discussing as reviewers the merits and potential shortcomings of the solution. Chronicled was then given a 2 month period to formally document the method for final review by the review panel. Coming out of this assessment, I believe that the final work product produced by the Chronicled team is mathematically proven to do the job: chain of custody without double-spend or leakage of data to partners or competitors.

Zaki Manian
Executive Director, Trusted IoT Alliance
Over the past year, I have served as a proposal grant reviewer for the Zero Knowledge Foundation, so, naturally I was very excited to be asked by Chronicled to review their zk-SNARKs implementation for pharma supply chain. During my years at SkuChain, I was involved in many supply chain use cases for blockchain and constantly bumped up against the requirement of privacy, which has not been adequately solved to date on any multi-company supply chain platform, blockchain or otherwise. It is clear that privacy is a key component for many supply chain problems and the lack of a solution has been holding back all of the industries. Chronicled's implementation of the zk-SNARKs technology solves this privacy problem, and when utilized to track prescription medicines, this method holds potential to save many human lives. This is unique because it is the first useful demonstration of a zk-SNARKs protocol that solves a completely different business problem than private value transfer pioneered in the Zerocash protocol.

Joint statement

Problem. *Managing and securing supply chains is notoriously complex because the many entities that take part in the chain (manufacturers, distributors, points of sale) are not willing to pool all their data in one place since that data contains sensitive business information. This implies that coordinating and keeping track of items moving along the supply chain is prone to both errors and attacks. How can one, in this setting, achieve authenticity, namely establishing that an item was manufactured, at some point in the past, by a vetted manufacturer?*

Chronicled. *Chronicled has developed a method to address this problem of maintaining a connected record without loss of sensitive information via a combination of blockchain technology and zero knowledge proofs. This method was implemented by Chronicled Lead Blockchain Engineer Maksym Petkus and Chronicled CTO Maurizio Greco.*

Ingredients. *Before discussing the method, we briefly recall what of these two notions are.*

- *Blockchain technology provides distributed algorithms that enable a set of mutually untrusting stakeholders to maintain an append-only ledger of transactions without having to rely on a central trusted party to store this ledger on behalf of everyone.*
- *A zero knowledge proof is a method that enables one party to publish a statement such as "given a public function F and public output y, I know a secret input x s.t. y=F(x)" without revealing any information about the secret input x.*

The method. *At a high level, the aforementioned method works as follows. The entities in the supply chain use blockchain technology to maintain a ledger of transactions. Informally, each time an item moves from an entity A to an entity B, the two entities collaborate to produce a transaction that, rather than containing information about the movement of the item from A to B, contains an encryption of this information as well as a zero knowledge proof that the ciphertext so obtain indeed corresponds to such information. This transaction is later posted to the ledger.*

All other entities can see this new transaction added to the ledger, and can verify that it attests to a movement of an item, without learning any information about who made the movement or what the item moved was. Crucially, if entity A tries to move an item both to entity B and entity C, one of the two transactions will not be accepted to the ledger because the protocol prevents the same item from being "double moved".

The above solution can be thought of as a simplified version of the Zerocash protocol, adapted to the problem of ensuring authenticity of items moving in supply chains. It has been efficiently implemented by leveraging zk-SNARKs, which are a particularly efficient type of zero knowledge proofs.

On the approach. *Addressing the problem of item authenticity in supply chains by using blockchain technology and zero knowledge proofs is natural because there are multiple mutually untrusting stakeholders each of which is not willing to share with all others information about their own movements. On the one hand blockchain technology enables transactions between two stakeholders to reach all others, and on the other hand zero knowledge proofs enable these transactions to be publicly verifiable without having to contain sensitive information.*