CHRONICLED SUPPLY CHAIN ZK-SNARK IMPLEMENTATION
CLEAN ROOM REVIEW FINDINGS
NOVEMBER 20, 2017

1. INDIVIDUAL STATEMENTS

Alessandro Chiesa
Assistant Professor, University of California at Berkeley
The Chronicled pilot marries blockchain and zk-SNARKs 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 the intended purpose, which was to establish a secure and connected record of custody while maintaining full privacy and without the potential for double-spend 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-SNARKs 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.

2. 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. The method was invented 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.