Blockchain Beyond Cryptocurrencies: A Real-World Use Case

A Non-Repudiable Supply Chain Tracking System

Filippo Bosi, Michele Cappelletti, Stefano Monti, Guido Ravagli
Imola Informatica
Imola (BO), Italy
e-mail: {fbosi, mcappelletti, smonti, gravagli}@imolainformatica.it

***Abstract*—Blockchains have recently emerged as an architectural style to overcome the intrinsic trust problem that arises when single central authorities are delegated the role to keep certification information for different parties and actors. By fueling a host of different cryptocurrencies, various forms of blockchains are revolutionizing the finance sector. However, blockchains are rapidly emerging outside of the finance sector, disrupting the business scenarios. This paper presents a novel Supply Chain Tracking system that eliminates fraud and counterfeits from a specific business sector, namely toner cartridge regeneration, where a recent European directive (and subsequent national regulations) has posed stringent limitations.**

Keywords-Blockchain; supply chain; tracking.

I. INTRODUCTION

In recent years, cryptocurrencies have paved the way for a new architectural model for distributed, decentralized (i.e., with no central authority/single point of failure) transactions based on so-called blockchains.

Due to their nature as a distributed, non-repudiable, non-centralized ledger, blockchain adoption has now extended well beyond cryptocurrencies and finance in general [1], and relevant use cases begin to emerge in disparate business sectors, specifically where challenging traditional central "trust" authorities open up new business opportunities [2][3].

Blockchain adoption in contexts other than cryptovalues is quickly gaining momentum, and may be disruptive both in technical and in business terms.

Blockchain architectural styles and implementations pose some stringent limitations as well, and taking them into account is crucial when planning their adoption in business contexts other than finance.

This paper presents an innovative approach to certification and tracking of cartridge regeneration process and logistics.

A recent European Union (EU) directive called Green Public Procurement (GPP) [16], and subsequent national regulations (e.g., the Italian Criteri Minimi Ambientali – CAM [17]) require Public Administrations to have a relevant share of the toner cartridges they buy be regenerated and supplied by certified providers.

However, nowadays toner cartridge regeneration suffers from a high level of forgery, and the verification of used toner cartridge life cycle (e.g., whether they have been refilled from certified partners or not) becomes nearly impossible.

Some studies report that in the last five years, original and refilled cartridge market share have both significantly dropped, in favor of a steady increase of cloned/fake cartridge (from 1% to 30%).

We partnered with Eco-Recuperi [4] – a major Italian player in the cartridge regeneration process, and we designed a Supply Chain Tracking System that eliminates the possibility to sell counterfeit cartridges as certified, recycled ones, thanks to the adoption of blockchain as a distributed notarization system for supply chain certification.

The rest of this paper is organized as follows. Section II describes related work and background knowledge. Section III details the business scenario and main business/technical requirements. Section IV addresses the process and architecture of our solution. Section V concludes this paper and summarizes our main findings.

II. BACKGROUND

This section provides some background knowledge about blockchains, and surveys their benefits, architectural styles and alternatives, and their growing business adoption in many business sectors.

A. Blockchain features, benefits, and issues

Blockchain architecture [5] is a network of computing nodes that share a common state. Blockchain architecture and protocols are designed so that at any given time, the majority of nodes should agree on the state of a blockchain itself.

Changes on the state of a blockchain are recorded as a series (chain) of transaction groups (block): each transaction relates to a specific user (identified by a unique identifier), and a specific point in time (timestamp).

Blockchain typically acts as a generic distributed ledger of transactions and guarantees some key characteristics that lend themselves well to our business case.

1) Non-repudiation: every transaction users register on the blockchain automatically becomes non-repudiable, e.g., once a transaction takes place, the user that actually performed the transaction will not, in any case, be able to refute its responsibility about the transaction itself;

 ISBN: 978-1-61208-644-6

2) Irreversibility: every transaction users register on the blockchain automatically becomes irreversible, e.g., users are not allowed to cancel/edit/undo a transaction;

3) Transaction timestamping: any transaction happens at a specific point in time, and blockchain records such instant in a non-modifiable, and always identifiable way;

4) Censorship resistance: single transactions and the status of a system as a result of a series of transactions cannot be denied, and are always publicly available and verifiable.

The above features make blockchains a distributed ledger that notarizes events, and makes them universally, perpetually accessible and non-repudiable.

B. Blockchain architectural styles

Blockchain is neither a specification nor a technology, and is rather considered a paradigm/architecture style.

The first blockchain specification was the Bitcoin one, released in 2008 [6] [7]; from then on, many other blockchain implementations have emerged, with very different characteristics.

The Bitcoin blockchain has been considered the reference implementation of the blockchain paradigm. The major capability to implement is to – statistically - solve Byzantine Generals Problem [8], that is a classic problem faced by any distributed system network. The Bitcoin original implementation is based on hashcash [9], a proof of work algorithm. It is a smart approach to reach distributed consensus, providing a strong protection from brute force attacks, achieving overall system reliability in the presence of a number of faulty processes.

A proof of work algorithm has two strong implications: it needs a high amount of energy to run and it makes it harder to deliver real-time results, since it is distributed among a large and ever-increasing number of nodes, and it is based on computation-intensive random processing. Due to these limitations, many attempts have been made since Bitcoin release, to avoid proof of work shortcomings. Those implications set strong limits on transaction throughput and significant operational costs of the network. Proposed solutions focus on performance improvement and cost decrease: the most significant changes focus on the centralization of the transaction validation process and on the adoption of a consensus algorithm that is not based on the computational brute force principle.

These 'improvement solutions' can be considered as some sort of relaxation of constraints of the original Bitcoin blockchain architecture; while those relaxations are not necessarily a limitation, they should be carefully taken into account when determining which blockchain style fits business requirements and context the most.

Categorization [10] can be made in order to simplify blockchain types understanding:

- 'Bitcoin-like' Blockchains: blockchains with distributed consensus algorithm and history of transactions persisted in a chain of mathematically linked blocks; those are the blockchains that implement the original idea of blockchain as it was proposed by Bitcoin and their focus is on transaction history immutability and consistency over transaction throughput;
- 'Enterprise' blockchains: characterized by a centralization of core functionalities like transaction validation, block creation, and naming service; focus is set on governance aspects such as access regulation and privacy mechanisms;
- Distributed Ledger Technology (DLT): state is shared among nodes of the network, but no chain of blocks is implemented. Other measures are set in order to enforce immutability of transactions, but focus is set on performance in order to reach near-real time information distribution in the network.

Blockchains - and DLTs - can also be categorized by governance model, i.e., the possibility to access the blockchain with or without the permission of a remote account issuing service:

- Permission-less: users independently create their own account using a deterministic process that ensures the account identifier is globally unique, enabling them to immediately access the blockchain. It is the typical approach of 'Bitcoin-like' blockchains;
- Permissioned: users registration has to be approved by the blockchain centralized service issuer, such as any traditional Information Technology (IT) service.

C. Blockchain use cases and business opportunities

As previously discussed, the blockchain paradigm addresses the big challenge of securely collecting events in a distributed scenario enhancing immutability, transactionality, and near-real time delivery; the following section describes real world scenarios that take advantage of the adoption of the blockchain paradigm.

First of all, the use case the whole world knows is the one the blockchain was born for: exchange of a new digital currency, both coined and exchanged inside the blockchain. The birth of the blockchain marks the introduction of a new type of currency, alongside traditional fiat currencies, where fiat means the currency has a legal value and is coined by a proper institutional entity.

Digital currency exchange use case has already many real-world business case, such as:

- Cross border money transfer: near real-time delivery of transaction in the network allows worldwide value transfer with significant time and cost decrease with respect to traditional processes;
- Pseudonymous [11] money transfer: as previously said, account creation can be done autonomously. In addition, account data are pseudonymous, which means accounts do not include any personal data. These two features allow enhancing privacy features in value exchange between users;

- Closed virtual currencies: since the blockchain enables issuing digital currency autonomously, organizations can take advantage of this feature to replace - or implement – closed loop exchange of value such as fidelity card for customer retention and food stamps for employers.

Notarization is a less explored use case for blockchains, and derives directly from three Bitcoin-like blockchain features, provided that they come together:

- Non-repudiation: transaction issuer cannot repudiate ownership of his transactions;
- Immutability: transactions inserted in the blockchain cannot be altered in any way after being considered validated;
- Timestamping: every transaction is timestamped with the blockchain time once considered valid by the network.

A blockchain implementing all those three features can be considered as a notary and transactions made on the blockchain can be considered as notarized events.

Many business cases and applications can enhance certification of their processes by enforcing trust using blockchain as a notary service: tracking processes phases on the blockchain means they become unmodifiable milestones. While few real world applications of this use case are already in production, the great majority are yet to come:

- Track phases of clinical trials [12];
- Track patents issuing, intellectual property and copyrights [13];
- Track supply chain of goods, such as the cartridge recycling process phases presented in this paper.

III. SCENARIO AND REQUIREMENTS

This section describes our scenario and requirements from both business and technical perspectives.

A. Objectives

The main business goal of this project was to provide a reliable/verifiable certification process for cartridges lifecycle, to limit regeneration frauds. This means being able to:

- track cartridge status change between the various stages of refill processes (e.g., collect, refill, package, distribute, sell);
- physically tag/associate each cartridge with such lifecycle information with easily readable, non-repudiable, and tamper-proof mechanisms;
- build a verification infrastructure that lets anyone publicly verify the status of each cartridge.

The verification infrastructure itself has stringent non-functional requirements:

- reliability and trust: the infrastructure should prevent anyone from introducing fake data to certify non-recycled cartridges;
- simplicity: to ease adoption, especially among Public Administrations;
- cost-effectiveness: physical tags and the associated verification process should pose a negligible cost overhead, to avoid posing refilled cartridges out of market;
- accessibility: the verification tools should be easily accessible, via e.g., Web Applications and Mobile Applications.

B. Actors and process

The main actors are:

- Certification Authority: independent actor that issues unique identifiers (UIDs) to tag and track refilled cartridges;
- Collector: economic subject that collects exhausted toner cartridges and selects them for regeneration;
- Refiller: economic subject that actually refills exhausted cartridges;
- Distributor: economic subject that distributes and sells refilled toner cartridges;
- Customers: private/public subjects that buy refilled cartridges;
- Recycling consortium: consortium of recycling supply chain participants whose recycling process has been reviewed and approved by the Certification Authority; any cartridge refilled from a Refiller of the Consortium is identified by a UID from the Central Authority.

Figure 1. Traditional cartridge recycling process and actors

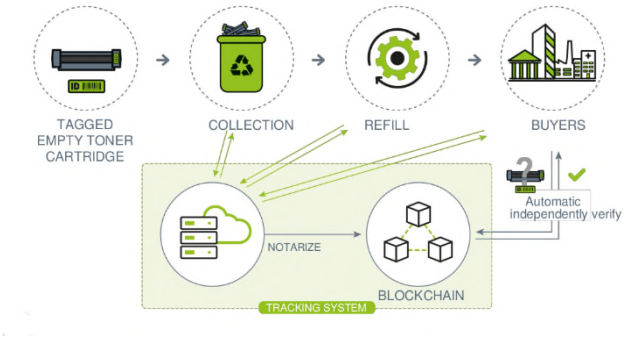

Figure 2. Blockchain-enabled, trusted recycling process and actors

Figures 1 and 2 depict traditional and blockchain-based processes, respectively.

The blockchain-based process steps are as follows:

- Step 0 – UID distribution: PACTO (Produttori Associati Cartucce e TOner) [18] Consortium distributes UIDs to certified Collectors, and keeps track of UID-Collector relationships;
- Step 1 – Cartridge collection: certified Collectors physically collect cartridges and cartridges, and tag them with physical, non-removable, low-cost medium (e.g., Near-Field Communication -NFC tags) that carry UIDs; from now on, each cartridge is uniquely identified by a UID and can be tracked throughout the whole process;
- Step 2 – Cartridge refill: certified Refillers receive exhausted cartridges from Collectors;
- Step 3 – (Optional) Cartridge Distribution: distributors are (optional) intermediary partners that facilitate cartridge sell;
- Step 4 – Sell: Distributors and Refillers are allowed to sell refilled, certified cartridges;
- Step 5 – Verification: Customers can verify cartridge refill process steps, from 1 to 4, hence being able to assess cartridge refill compliance.

C. The key blockchain role

From step 1 onwards, each step advance can be tracked and uniquely associated to a physical cartridge.

A traditional, centralized database of cartridges does not meet reliability and trust requirements: the owner of the database may easily alter database content, leaving other parties no option to verify the correctness of cartridge information.

This inherently distributed update and verification process lends itself well to the adoption of a blockchain-based approach; in our model, blockchain acts as the distributed, decentralized ledger that:

- keeps track of cartridges status advances, and uniquely identifies them (and each status change) via their UID;
- allows any party to verify each stage of the refill process, at any time, and with no option for anyone to alter/fake them.

D. Blockchain choice

Blockchain choice was a core activity of the analysis phase of the project. A huge effort has been spent on studying and researching to understand pros and cons of major public blockchain implementations. This phase was hard, because we were not even aware of the Key Performance Indicators (KPIs) to use for the evaluation. The blockchain is not just a software component: even the community surrounding it, which is defining its evolution roadmap has strong implications on several key aspects that have to be taken into consideration during the evaluation phase. Legal implications, constraints on the underlying service design, community principles, and so on, have to be included in the evaluation.

Key aspects to evaluate are:

- How the business service is considered critical: the most important element is understanding how service delivery failures can affect the real world. For example, using the blockchain in healthcare could be highly critical for humans, in supply chain or copyright protection it could result in considerable penalty to pay, and so on. In order to reasonably guarantee a reliable service, it is necessary to focus on the maturity level of the blockchain implementation, and the level of reliability of its distributed service network. On the other hand, if blockchain is used for a less critical use case, such as academic research, it is safe to adopt less mature technologies;
- Requirements on blockchain governance: should the access be regulated or not? Focus has to be set on governance processes at business level;
- Requirements on data to be written on the blockchain: first of all, data written on the blockchain are intended to be stored publicly, immutably and forever; this implicit feature has strong implications on privacy and data lifecycle, particularly if the blockchain is deployed and used in a public scenario;
- Requirements on performance and integrations: performance common KPIs are transaction validation time, transaction delivery throughput, and scalability of the blockchain; integrations aspects focus mostly on the quality and maturity of integration tools such as library and development environments;
- Cost of the blockchain infrastructure: blockchain costs can be divided in costs of transactions issued, intended as the fee related to those transactions and costs needed to run the infrastructure, intended as computational power to run nodes of the network,

 ISBN: 978-1-61208-644-6

computational power to generate the blocks, and other costs related to connection handling such as bandwidth.

Ultimately, a wider understanding and weighted evaluation on several aspects discussed above had led to consider the Bitcoin blockchain the best choice for this use case.

IV. ARCHITECTURE

The following section describes our Supply Chain Tracking System architecture main inspiring principles and design choices.

A. Architecture principles

Blockchain, as a distributed verifiable data storage, suffers from two main issues:

1. costs: registering transactions (events) on a blockchain usually has non-negligible execution times and transaction fees (costs), especially on public, permissionless blockchains;
2. storage space: Bitcoin blockchain allows storing custom payloads of 80kb: this means storing business-related pieces of information on blockchain is usually infeasible for real-world scenarios.

Due to the scope of our business scenario, we expect the number of transaction registrations to exponentially grow over time, since it depends on the number of certified refilled cartridges and on each status update event. In our model, transaction fees become a direct, proportional cost that contributes to the final cartridge price (as of today, this fee is upon the consortium itself). This is the main reason why cost efficiency throughout the whole recycling process is key in keeping refilled cartridges market-competitive, and we had to design a way for transactions on the blockchain to remain cost- and time-effective, no matter the increase in number of events. Our solution addresses both issues by adopting three key tenets.

First, we define an Event Common Tracking Model (ECTM) - a minimum set of pieces of information that each actor on the process agrees upon to keep track of cartridge status changes; this allows keeping business information strictly needed for notarization to a minimum, and contemporarily enabling interoperability between actors of the supply chain.

Second, we delegate storage of business information to traditional databases: Business Databases can either be centralized (e.g., a single database for the consortium) or distributed (e.g., each actor may have its own database). The only requirement on such databases is to keep track of the Common Tracking Model for each.

Third, to obtain cost efficiency and throughput, we group a set of multiple events into a single blockchain transaction; each group has the following characteristics:

- Each ECTM in a group gets hashed in an Event Hash (EH);
- Event Hashes are combined and hashed together via a Merkle-tree algorithm, producing a Group Hash (GH); this Merkle-tree-based approach is quickly becoming a major solution to provide a reproducible, hash based event grouping mechaninsm for blockchain efficiency, and is currently being adopted by a number of online blockchain based services, such as Eternity Wall [14] – the blockchain-based public message wall that promises messages lasting forever on the blockchain itself;
- The Group Hash gets stored on the blockchain.

This approach guarantees the following features:

- Flexibility: actors can save any business-related information into the Business Databases, provided the Common Tracking Model information are stored;
- Non-repudiability: any party that owns or knows a Common Tracking Model for an event, can easily verify against the blockchain its correctness; having Common Tracking Models hashed on the blockchain guarantees this model is tamper-proof and unmodifiable.

B. Architecture description

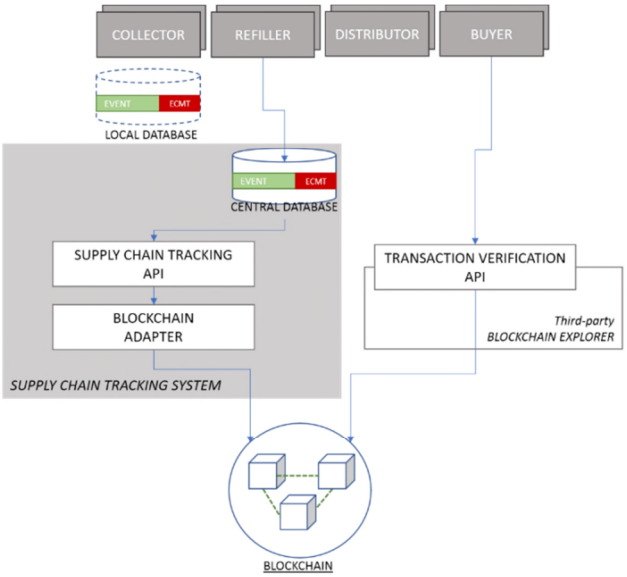

Figure 3. Architecture

Our Supply Chain Tracking System (see Figure 3) is based on the components described below.

Business database(s): in our first implementation, the PACTO Consortium holds a central database where business information related to recycling events are stored for any involved party; these is no need for this kind of

database to be central, and any single operator of any kind can adopt its own local database.

Transaction storage: this component holds the aggregation and hashing logic described in section IV.A

Blockchain adapter: this component acts as an abstraction layer that hides blockchain-specific transaction registration details, so as to let the architecture be portable between different blockchain implementations;

Blockchain Explorer: third-party service that allows to view information about blocks, addresses, and transactions on the Bitcoin blockchain. Our implementation relies on the open source Web portal BlockExplorer [15].

V. CONCLUSION AND FUTURE WORK

This work presents a novel Supply Chain Tracking System that relies on Bitcoin's blockchain to realize a notarization system supply chain goods status change and transitions.

This solution allows to overcome traditional fraud and counterfeit problems in a specific business sector, namely toner cartridge regeneration.

Future work will focus on investigating some new models and mechanisms (such as Lightning Network [19]) to keep Bitcoin's blockchain purest model, and simplify and speed up registration of transactions on the blockchain itself.

ACKNOWLEDGEMENT

This research was supported by Eco-Recuperi staff, whose insight and expertise greatly assisted the research, design and implementation of this work.

REFERENCES

[1] World Economic Forum, *The Future of Financial Infrastructure*, [Online] Available from: http://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services [retrieved: 2018.06.01]

[2] T. Aste, P. Tasca and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," in Computer, vol. 50, no. 9, pp. 18-28, 2017. doi: 10.1109/MC.2017.3571064

[3] M. Swan, "Blockchain: Blueprint for a New Economy", O'Reilly, 2015.

[4] Eco-Recuperi, *Eco-Recuperi website* [Online]. Available from: http://www.ecorecuperi.it/ [retrieved: 2018.06.01]

[5] A. Anjum, M. Sporny, and A. Sill, "Blockchain Standards for Compliance and Trust" in IEEE Cloud Computing, vol. 4, no. 4, pp. 84-90, July/August 2017. doi: 10.1109/MCC.2017.3791019

[6] S. Nakamoto, Bitcoin: *A Peer-to-Peer Electronic Cash System*, [Online] Available from: https://bitcoin.org/bitcoin.pdf [retrieved: 2018.06.01]

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton Univ. Press, 2016.

[8] L. Lamport, R. Shostak, and M. Pease. 1982. "The Byzantine Generals Problem".ACM Transactions on Programming Languages. Syst. 4, 3 (July 1982), 382-401.

[9] A. Back, Hashcash – *A Denial of Service Counter-Measure*, [Online] Available from: http://www.hashcash.org/papers/hashcash.pdf [retrieved: 2018.06.01

[10] A. Lewis, *A Gentle Introduction to Blockchain Technology*, [Online] Available from: http://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Bitcoin-WEB.pdf. [retrieved: 2018.06.01]

[11] *Protect your privacy*. [Online]. Available from: https://bitcoin.org/en/protect-your-privacy [retrieved: 2018.06.01]

[12] Kodak. *Kodak Cryptocurrency and Blockchain Ledger Will Help Photographers Protect Their Copyright* [Online]. Available from: https://futurism.com/kodak-cryptocurrency-blockchain-ledger-help-photographers-protect-copyright/ [retrieved: 2018.06.01]

[13] *Distributed Ledger Technology in Clinical Trials* [Online]. Available from: https://tokeneconomy.co/distributed-ledger-technology-in-clinical-trials-fc2284bbe533 [retrieved: 2018.06.01]

[14] Eternity Wall, *How to independently verify notarization?* [Online] Available from: https://blog.eternitywall.com/2016/05/16/how-to-independently-verify-notarization/ [retrieved: 2018.06.01]

[15] Block Explorer [Online] Available from: https://blockexplorer.com/[retrieved: 2018.06.01]

[16] European Commission, *Green Public Procurement* [Online] Available from: http://ec.europa.eu/environment/gpp/index_en.htm [retrieved: 2018.06.01]

[17] Ministero dell'Ambiente e della Tutela del Territorio e del Mare, *Criteri Minimi Ambientali* [Online] Available from: http://www.minambiente.it/pagina/i-criteri-ambientali-minimi [retrieved: 2018.06.01]

[18] Associazione PACTO [Online] Available from: http://www.associazione-pacto.it/ [retrieved: 2018.06.01]

[19] Lightning Network [Online] Available from: https://lightning.network [retrieved: 2018.06.01]

 ISBN: 978-1-61208-644-6