System and Methods for Blockchain-Inspired Digital Game Asset Management

Gianluca Ragnoni

Abstract In 2017, IGT's Italian Software Architecture team, identified some features of the emerging blockchain, as enabling technologies to manage a ledger (or data store) that used cryptography and digital signatures to prove identity and authenticity (G. Ragnoni, E. Martire, F. Battini, *System and Methods for Blockchain-Based Digital Lottery Ticket Generation and Distribution* USPTO, Application Number 15/916,620 Filing date Mar 9 2018. https://patents.google.com/patent/US10931457B2). The idea was to design and implement a fully managed ledger database that provided a transparent, immutable and cryptographically verifiable platform for managing the creation of digital assets (e.g. game ticket) and the transfer of asset's ownership between users. Following the above idea, the team designed and implemented Transaction Certification Authority (TCA), an IGT platform that tracks each and every asset's transactions and maintains a complete and verifiable history of ownership change over time. The aim of this paper is to present TCA, its features and functioning mechanism.

Keywords Blockchain · Asset management · Digital game

1 Context and Concepts

The digitalization era is highlighting new opportunities to enhance customer experiences, providing new advanced, personalized, tailored and improved services for all actors involved into the Gaming Value-Chain [1].

Within this context, IGT built a digital gaming vision intending to unleash in-store digital experiences providing new digital journeys for customers within the Point of Sales. In this scope, IGT already provided several digital services to the customers enabling to get info, filling playslip, checking winnings through digital

G. Ragnoni (✉)
IGT, Rome, Italy
e-mail: gianluca.ragnoni@igt.com

A. Masone et al. (eds.), *Optimization and Data Science: Trends and Applications*,
AIRO Springer Series 6, https://doi.org/10.1007/978-3-030-86286-2_14

touchpoints (e.g. mobile devices, self stations, etc.). In addition, mixed paper-digital services have already been provided enabling customers to participate to a digital lottery starting from a paper.

With the aim to have a full in-store digital experience the main challenge is related to provide the ability to manage digital tickets maintaining:

- The gaming model currently in place, where customers are not obliged to open game account to participate to the Lottery;
- The advanced security and anti-tampering measures integrated on the paper tickets.

Exploiting some features of the emerging Blockchain model [2, 3], IGT designed and developed a proprietary digital asset management solution called Transaction Certification Authority (TCA) for digital ticket management.

TCA is a fully managed ledger database that provides a transparent, immutable and cryptographically verifiable platform for managing the creation of digital assets and the transfer of assets' ownership between users. With TCA, the transaction's change history is immutable, it cannot be altered or deleted, using cryptography, and the client can easily verify that there have been no unintended modifications to asset's ownership.

The article is structured as follows: in Sect. 2 the TCA systems are described in terms of Scenario, Actors and Concept and Transactions available; in Sect. 3, the security requirements addressed by project referring to security standards are summarized; Sect. 4 is devoted to conclusions.

2 TCA

In this section the TCA systems are described in terms of Scenario, Actors and Concept and Transactions available.

The first subsection describes the main use case introducing a logical model to address the business requirements, the second subsection details the model of the project in terms of actors of the system, actions (or transaction) that each actor can do, rules of the actions, finally the type of transactions available in the system are explained using interaction diagrams.

2.1 Scenario

TCA is a platform designed to certify the ownership of arbitrary digital assets, regarding asset issuing and asset transferring between users, ensuring anonymity of the users, confidentiality, data integrity, non-repudiation, process transparency and reproducibility.

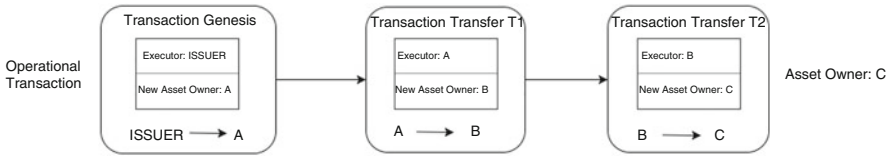

Fig. 1 Scenario A

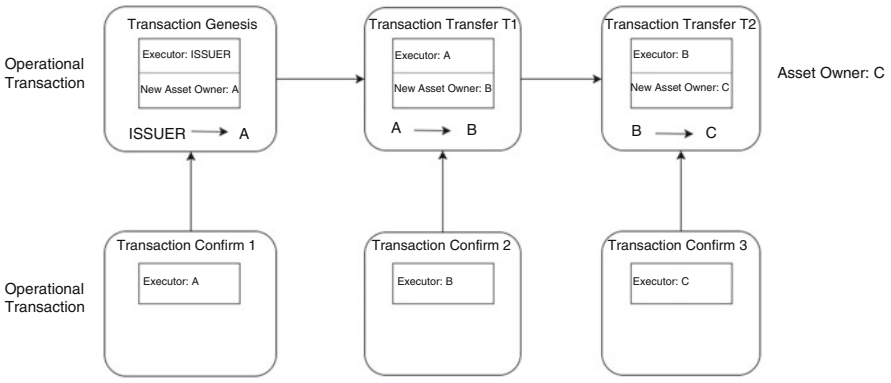

Fig. 2 Scenario B

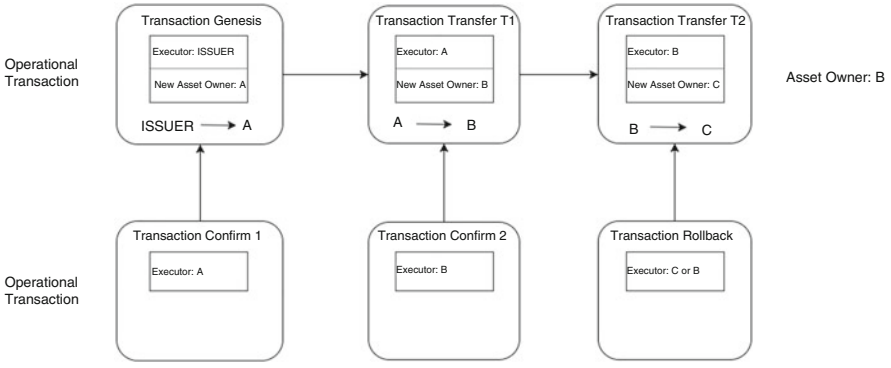

Fig. 3 Scenario C

By means of TCA a client with a specific clearance can register an asset on TCA; after registration users can transfer assets each other.

The TCA allows *implicit agreement* or *explicit agreement* when a new owner receives a digital asset: if the agreement is implicit (explained in the example in Fig. 1) when a digital asset is transferred to him, he automatically becomes the new owner, instead if the agreement is explicit (explained in the examples in Figs. 2 and 3) he may confirm or deny (rollback) the transfer.

2.2 Actors and Concepts

TCA adopts a model involving the following **actors**:

(i) The **Issuers**: the actors issuing digital assets;
(ii) **Clients**: the actors owning and transferring assets;
(iii) The Transaction Certification Authority (**TCA**);
(iv) One or more external Certification Authority (**CA**), used as a trusted third party external entity to guarantee immutability.

Each actor has a pair of asymmetric keys and it is identified by its public key (pubkey).

Issuer and customers interact through transactions.

2.3 Transactions

There are two types of **transaction**:

Operational Transaction Invoked by the subject issuing or transferring the asset; it allows to record the new ownership of the asset. Each transaction is the transfer of ownership of a digital asset (**DA**) from a public key called *SOURCE*, to another public key called *DESTINATION*. Each transaction is linked to the previous owner through the transaction hash.

- **Genesis Transaction**: this transaction allows to register an asset on the *TCA* and assigns its ownership to a client. It is always invoked by the *Issuer*.
- **Transfer Transaction**: allows to register the transfer of an asset from the current owner to a new owner.

Control Transaction If enabled, it is invoked by the client that receives an assets or, in case of rollback, by one any of the clients involved in the transfer, to confirm or deny the change of ownership. Each control transaction is linked to the operational transaction to be confirmed or rolled back.

- **Confirm Transaction**: this transaction allows the destination to confirm the willingness to receive the asset.
- **Rollback Transaction**: this transaction allows the destination to reject the asset or the source to abort the transfer if the destination has not confirmed it yet.

Each transaction is authorized by the TCA and the *SOURCE* using a digital signature.

Each transaction is recorded also in a block in a public transaction ledger (**PTL**) by TCA.

Each block is hashed and is linked to the previous block via hash value in the PTL.

Each block hash is also timestamped with a signature provided by CA. This feature guarantees the immutability via an external trusted third party entity.

Examples:

- **Scenario A**: in Fig. 1, control transaction disabled (implicit agreement). Only operational transaction. The final owner of the digital asset is C.
- **Scenario B**: in Fig. 2, control transaction enabled (explicit agreement), with confirm transactions. The final owner of the digital asset is C.
- **Scenario C**: in Fig. 3, control transaction enabled (explicit agreement), with confirm and rollback transactions. The final owner of the digital asset is B.

Figure 4 depicts a sequence diagram showing the message flow of Genesis Transaction with implicit non-repudiation. Genesis Transaction has three actors: a customer (Customer1) requiring an asset generation from an authorized issuer (Issuer) that generates the asset, the TCA as a digital notary to guarantee issuing, transfer and ownership of the digital asset.

In message #1 Customer1 requires asset issuing to the Issuer, specifying his public key as the destination for the asset.

In message #2 Issuer creates a digital asset (DA) and creates a message (MSG) contains DA, the origin of DA (or the source) inserting his public key and the destination of the asset using the public key received from the Customer1.

In message #3 Issuer signs MSG with his private key (DS Issuer).

In message #4 Issuer sends MSG and DS Issuer to the TCA.

In message #5 TCA does a set of checks as for example if the Issuer is authorized to issue the asset, if asset is new and it is well formed syntactically etc . . . If checks are positive, TCA signs MSG (DS TCA), creates a new transaction with MSG, DS Issuer and DS TCA and saves the transaction in the Public Transaction Ledger (PTL).

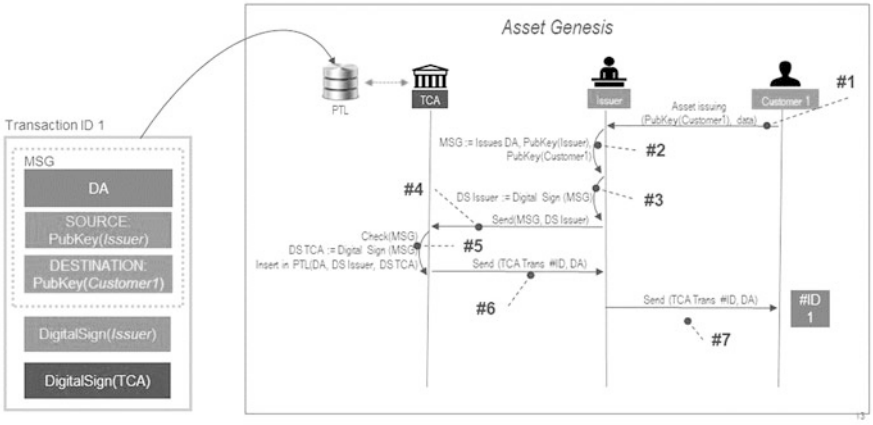

Fig. 4 Genesis transaction

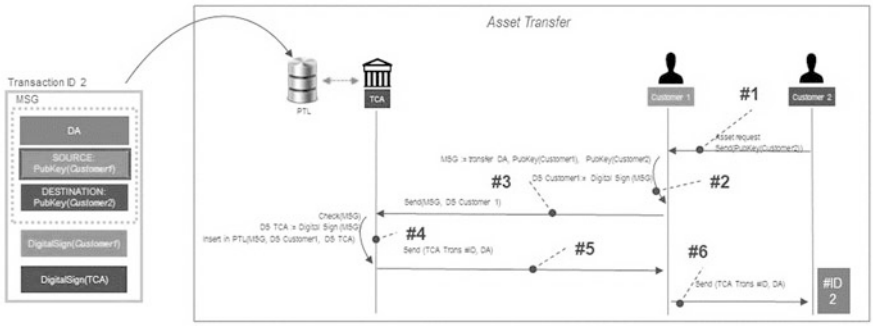

Fig. 5 Transfer transaction

In messages #6, #7 transaction is sent back to Issuer and to the Customer1. At the end of this process, Customer1 is the owner of the asset.

Looking at the Transaction ID1 to the left of the diagram, we can see the message (MSG) containing the asset (DA), the issuer of the asset (or SOURCE) represented by the public key of the Issuer, the owner of the asset (or DESTINATION) represented by the public key of the Customer1. Then the message signatures made by the Issuer and by the TCA.

Figure 5 depicts a sequence diagram showing the messages flow of Transfer Transaction with implicit non-repudiation. A typical Transfer Transaction has three actors: a customer (Customer2) requiring the transfer of an asset from another customer (Customer1) that owns the asset and the TCA that acts as a digital notary to guarantee correctness of transfer and new ownership of the digital asset. In the Transfer Transaction the current owner of the asset (SOURCE), has the right to transfer the asset to someone else (DESTINATION).

In message #1 Customer2 requires an asset transfer to Customer1 specifying his public key as the new destination of the asset. In arrow #2 Customer1 creates a message (MSG) contains DA, the origin of DA (or the source) inserting his public key and the destination of the asset using the public key received from the Customer2. Customer1 signs MSG with his private key (DS Customer1).

In message #3 Customer1 send MSG and DS Customer1 to TCA.

In message #4 TCA does a set of checks as for example if the Customer1 is the current owner of asset and has the right to transfer. If true, TCA digital sign MSG (DS TCA), creates a new transaction with MSG, DS Customer1 and DS TCA and saves the transaction in the Public Transaction Ledger (PTL).

In messages #5, #6 transaction is sent back to Customer1 and to the Customer2. At the end of this process, Customer2 is the owner of the asset.

Looking at the Transaction ID2 to the left of the diagram, we can see the message (MSG) containing the asset (DA), the previous owner of the asset (or SOURCE) represents by the public key of the Customer1, the current owner of the asset

(or DESTINATION) represents by the public key of the Customer2, the message signatures made by the Customer1 and by the TCA.

3 Security Features

According to the standard **ISO/IEC 27000:2018** [4], information security is the protection of confidentiality, integrity, availability (often denoted by acronym CIA); the same standard also includes other requirements, as authenticity, accountability, non-repudiation, and reliability. In the well-known glossary CNSS [5], data security is described according to the CIA requirements: "*The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability*".

The definition in the ISACA [6] glossary is similar: "*Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).*"

In the framework of the TCA project, among the ISO/IEC 27000:2018 requirements, we select as relevant, the following items to implement:

- Confidentiality: information is not made available or disclosed to unauthorized individuals, entities, or processes;
- Integrity: information is complete and correct, in particular, information cannot be modified in an unauthorized or undetected manner;
- Authenticity: each entity involved in some operation should provide a proof that it is what it claims to be;
- Non-Repudiation: each entity involved in some operation cannot deny having executed its own actions.

Other requirements are not managed directly, since they are implied by the previous ones (accountability is implied by integrity, authenticity and non-repudiation), or they are out of the scope of this study (availability, reliability).

4 Conclusion

In the gaming context, TCA platform can enable ticket receipt dematerialization inside the retail store with a seamless integration with current ecosystem providing a "Phygital" (physical and digital) experience for the user that can have a digital version of ticket receipt (the asset) in their mobile device, with the same security features of the physical one.

Moreover TCA, can play the role of "layer 2 infrastructure" integrating itself with a public blockchain infrastructure. In fact, since 2017, public blockchain infrastructures have been evolved and nowadays, although there are a lot of blockchain

available, capable to manage directly arbitrary digital assets, according to experts and community thoughts [7], specific domain applications will be necessary on top of blockchain, in order to manage specific digital assets in a scalable way. Playing this role, TCA could be a specific domain application that manages digital tickets for gaming companies that want to enable ticket receipt dematerialization. In this scenario, public blockchain infrastructure can replace the Certification Authority saving only block's fingerprint of transactions managed by TCA.

TCA model has been patented [8] in US with number US10931457B2 and is already integrated in the Italian Digital National Lottery.

References

1. The World Lottery Summit 2018—Jean Jorgensen Merit Award for Innovation—"Lottomatica Lottery Ticket Digitalization Based on Blockchain Model"
2. Bitcoin: A Peer-to-Peer Electronic Cash System—Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf
3. Blockchain Series (MOOC)—University at Buffalo School of Engineering and Applied Sciences. https://www.coursera.org/learn/blockchain-basics
4. ISO/IEC 27000:2018. ISO/IEC 27000:2018. https://www.iso.org/standard/73906.html (2018)
5. Committee on National Security Systems. National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 Apr 2010. https://www.hsdl.org/?view&did=7447
6. ISACA. Information Systems Audit and Control Association. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (2021)
7. 102 blockchain leaders share their insights into the use of blockchain both now and into the future. Taken from https://zage.io/report/pdf/blockchain-102.pdf
8. Ragnoni, G., Martire, E., Battini, F.: Systems and methods for blockchain-based digital lottery ticket generation and distribution. USPTO, Application Number 15/916,620—Filing date 9 Mar 2018. https://patents.google.com/patent/US10931457B2