Blockchain based Proof-of-Ownership protocol

This paper outlines how blockchain and NFT (Non-Fungible Token) can be used to prevent counterfeit. NFT is a unique and non-interchangeable crypto asset store on blockchain; it can be used to represent physical objects.

Authentic material good: material good produced under the control of the legitimate manufacturer, originator of the good or holder of intellectual property rights. (ISO 12931:2012).

Title token: brand owners need to issue a NFT for every single object they are authorized to produce when using blockchain based proof-of-ownership protocol. NFT is the true authentication element stored on blockchain, the primary instrument to proof ownership, thus the name of the title token.

Authentic good: should making up with three parts:

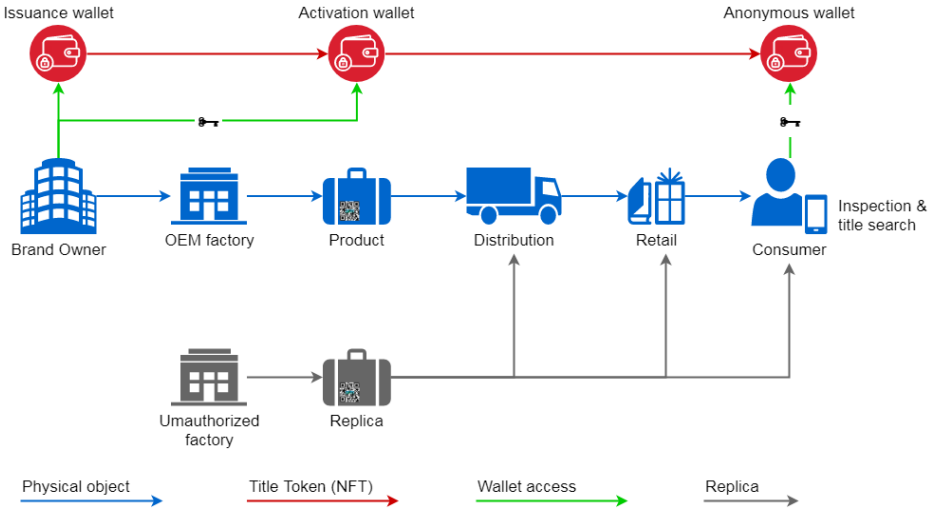
1. Physical object
2. Authentication label, suggest using QR code to print title token ID
3. NFT, aka title token, resides on blockchain

Counterfeit good: a complete set of counterfeit good should also include three parts:

1. Replica of physical objects. Difficulty level – normal.
2. Replica of authentication label. Difficulty level – normal.
3. Replica of title token. Difficulty level – **impossible**, unless the strong encryption of SHA-256 is cracked.

Anti-counterfeiting logic: product with title token issued by brand owner is authentic; otherwise counterfeit. (The title token stored on blockchain, not the code or label.)

Creation and transfer history of a title token is recorded on blockchain by digital wallets. Each wallet is protected by strong encryption, exclusively used by the private key holder. Deceptive products placed into the supply chain can be easily identified by blockchain based title search. (Please search title toke ID 9990048413986158969 at CryptoC14.com for demonstration)

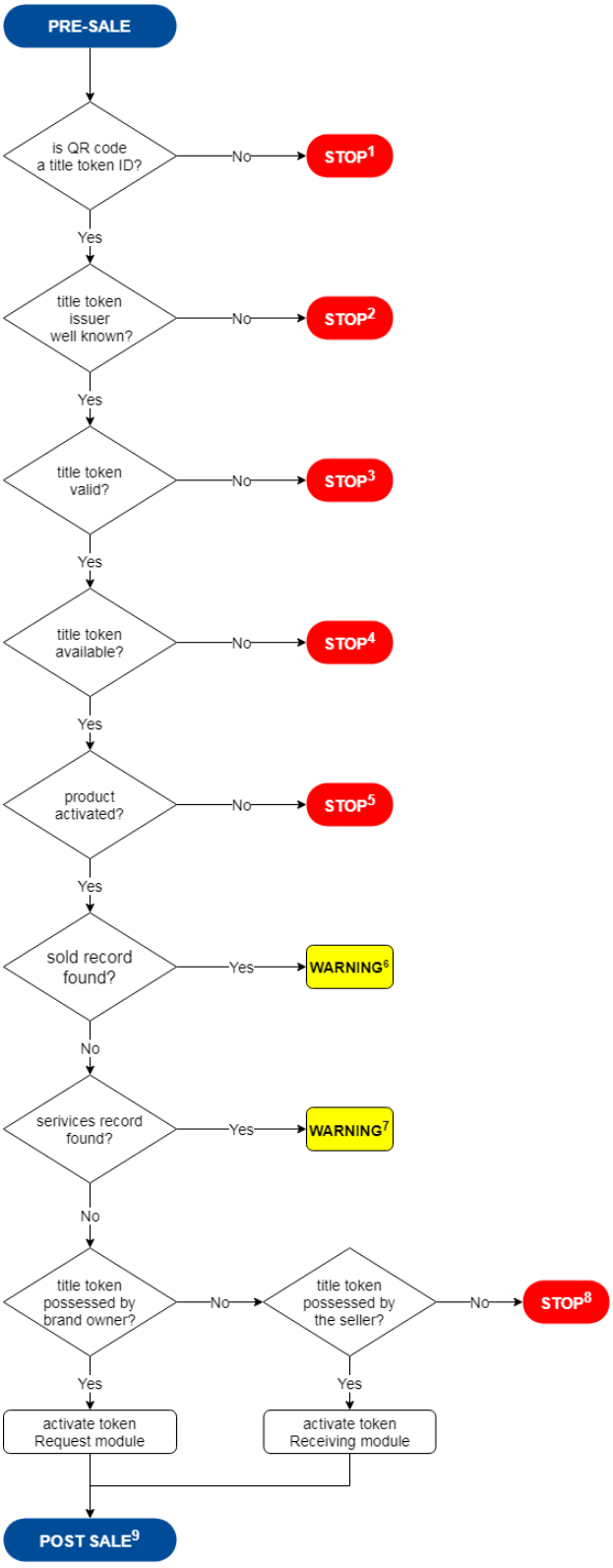


By CC14-49CE-CXZZ-3QHW-AH4JK

Blockchain based title search: this is not a traditional title search; it mainly focuses on the ownership history of authentic goods. It may include financial analysis in future.

Consumers use blockchain based title search to verify the origin of a product and identify its current owner. Protected by blockchain technology, no matter how many replicas were made physically, there are a limited number of title tokens issued by brand owners that can be bundled with.

1. Sign of counterfeit. Product without title token is not protected by blockchain based Proof-of-Ownership protocol. (Search any numerical code at CryptoC14.com)
2. Sign of counterfeit. Unable to identify the brand owner of an unknown wallet address. (e.g. 130725379765346402)
3. Sign of counterfeit. Title token was issued after the issuance wallet was set to expire by the brand owner.
4. Sign of counterfeit. Title token was destroyed by latest owner due to product failed QC test, lost, damaged, contamination, etc. (e.g. 8979558791471997978)
5. Sign of counterfeit. Corresponding product was authorized to build but not activated for distribution or sale. Final product shouldn't be found outside of the factory without activation. (e.g. 9515666061890261866)
6. Sold record found. Every time the title token stored in an anonymous wallet is considered sold. Items might suffer from the trick known as new-wine-in-old-bottle. Stay away if possible. Note, a known wallet address to brand A may be an unknown address for brand B. Any record found other than trusted wallet is considered as sold. (e.g. 16451992241381698202)
7. Service record found. Warranty might shorten due to services. Stay away if possible.
8. Sign of counterfeit. Seller cannot prove he has the right to convey the authentic goods.
9. Depending on who possessed the title token, consumers either claim the token by using an online tool offered by the brand owner, or they should receive the token from the seller directly. Authentic verification apps will activate correct tools based on title search result. Law enforcement should skip this step. Optional for distributors and retailers.



(Note: title search has nothing to do with physical characteristics. It is all about the collection of rights granted by brand owners, such as the rights of use, resale, warranty services, return, exchange, etc. Similar systems can be found in real estate and auto industries. However, the traditional title recording system is too slow and high cost.)

By CC14-49CE-CXZZ-3QHW-AH4JK

Performance: title search and transfer can be completed from less than a second to under a minute, depending on solution provider and blockchain platform.

Cost: free for consumers to use. Brand owner's cost in the range of $0.05 to $0.35 per title token per item, including blockchain transaction fee.

User experiences: depends on solution. At CryptoC14.com, consumers can finish authentic check, title search and claim title token by no more than three QR codes, way fewer keystrokes then booking a ride. Operators of brand owners can manage title tokens without programming knowledge. Web forms and dropdown menus are capable of handling most daily operations such as token issuance, activation, burning (destroy title token for damaged product).

Privacy: consumers use anonymous wallets to collect title tokens, normally built-in with authentication applications. Consumer's real identity will never be used by blockchain based Proof-of-Ownership protocol. The only personal information known to the public is the anonymous wallet address. Consumers may use multiple wallets to fragment their shopping pattern. Brand owners on the other hand, must reveal their wallet addresses dedicated for token issuance, activation, etc. to provide traceability.

Comparison: comparison between physical authentication, track & trace and proof-of-ownership is shown below. Text highlighted in red is the disadvantages of given technologies.

	PHYSICAL AUTHENTICATION	TRACK & TRACE	PROOF-OF-OWNERSHIP
Authentication Element	Label, chemical, mechanical, fingerprint devices …	QR code, RFID, IC …	QR code
Reading device	Bare eye, analyzer…	Smart phone	Smart phone
Professional skill	Required	No required	No required
Traceability	No[1]	Yes	Yes
Connection to server	Traditional DB	Traditional DB/Blockchain	Blockchain[4]
Anti-tampering	No	Yes/No[2]	Yes
Clone-proof	No	No[3]	Yes
Anti-counterfeiting logic	Outdated[1]	Weak, backfire[3]	Strong[5]
Total acquisition cost	Low/High	High[7]	Low[6]

1. Physical authentication lacks traceability. The best possible result is able to identify the manufacturer of an authentication element (e.g. Label). The relationship between the given label and brand owner of the genuine good is either implied (by trademark) or external (by database uses for fingerprint type of solution). Conclusions based on physical analysis are most likely to be misleading due to the global supply chain.
2. Depends on how the authentication data is generated. E.g. The IMEI generator is freely available for all phone manufacturers.
3. Track & Trace technology is able to identify where an authentic user should not be. It cannot prevent a replica being sold at the right place, since the authentication element is just a data point; it can be digitally cloned. To prevent this type of fault, solutions draw conclusions based on the number of times the data has been accessed:

if accessed more than once then there is counterfeit. The counting method can cause backfire. Authentic goods may be misjudged as counterfeit only because a customer scanned the authentication code twice. Other solutions covered the authentication code with destructive material to prevent accidental scanning; only paid customers can access the code. Unfortunately covert code also denies presale authentication.

4. Blockchain offers two significant advantages when used to prevent counterfeit compared to traditional database. Irreversible ledger and decentralized/distributed database. Data manipulation is virtually impossible in a well implemented blockchain network. Unlike centralized databases, users are required to set up accounts in order to access write permission. Public blockchains are normally fee based. Users pay a transaction fee in utility token to get write permission. (Different between writing a check vs. using paper money). Producing authentic goods is a centralized process initialized by its brand owner; however, the conveyance of a property is a decentralized process for most of time. The characteristics of blockchain and its fee paying model of access, along with NFT allow brand owners to tokenize authentication data without worry of it being tampered. Consumers on the other hand, can contribute to establish a trust network with brand owners without the hassle of account setup and risk of privacy breach.
5. Product with title token issued by brand owner is authentic; otherwise counterfeit. Title token (NFT) is clone-proof and exclusively possessed by some of the strongest encryption in the world. As long as the encryption algorithm used remains safe, this anti-counterfeiting logic is unbreakable.
6. Point to point method to transfer NFT is used by CryptoC14.com. Compared to relying on a chain of trusted entities to do the job, point to point data collection can dramatically reduce the total acquisition cost. Only brand owners and consumers get involved into the process, minimum hardware/software upgrades and personal training are required. A patent pending zero knowledge proof is used by CryptoC14.com to build trust between brand owners and their unknown consumers. Combined these two methods not just reduce total acquisition cost; it's also reduce the risk of data fault and errors.
7. Chain of data collection is a key element for Track & Track technology. It also inherits the drawback of this method[6].