fQR Weave lightpaper

https://fqrweave.tech

C.Tech
11/1/2020

Content:

1. Introduction:

Counterfeits are illegal products that are produced and commercialized in violation of a trademark, copyright, patent or other intellectual property rights (IPRs). Trade in counterfeit goods can cause damages to companies, slow economic growth and alter global competition. It also poses potential threats to the safety of citizens, in the form of goods that elude safety controls and regulations, and aliment criminal.

In February 2017 the International Trademark Association (INTA), along with the International Chamber of Commerce – Business Action to Stop Counterfeiting and Piracy, released a report from *Frontier Economics* entitled "The Economic Impacts of Counterfeiting and Piracy", quantifying the economic and social costs of counterfeiting and piracy. This report was unique, as it looked back at the global and domestic state of counterfeiting and piracy in 2013 and projected out to 2022. The report confirms that counterfeiting is growing globally and has a huge impact on the economy and society.

In 2013 the estimated value of international and domestic trade in counterfeit and pirated goods was $1.13 trillion. In 2022 the total estimated value of counterfeit and pirated goods, including digital piracy, is projected to reach $1.90 to $2.81 trillion. The number of legitimate jobs lost as a result of counterfeiting and piracy is estimated to reach 5.4 million by 2022. The global anti-counterfeiting trade is growing; stakeholders must work together collaboratively to combat it.

2. About Arweave:

Overview: Arweave is a data storage protocol built on blockweave technology. Arweave is developing an underlying network where data can be stored forever and accessed on its permaweb, a secondary layer where data is accessible in a human-readable manner (e.g. via web browsers).

Consensus: Arweave intends to use Proof of Access for its blockweave data structure to prove data is stored securely over time within its network. Proof of Access randomly selects a prior block – termed the recall block – and mandates that miners are able to provide specific data from the recall block (e.g. the block list hash). This process occurs for each block in the blockweave structure.

Blockweave and Proof of Access : Arweave's protocol combines a new data structure called a "blockweave" and a new consensus mechanism termed Proof of Access (PoA). As the name suggests, the blockweave protocol utilizes a block-based structure where each block is linked to two blocks.

Node Architecture: The protocol introduces variances to Bitcoin's node structure in which each node stores a block hash list – a list of the hashes of all previous blocks – designed to allow old blocks to be verified. Additionally, nodes possess a wallet list which contains a list of all "active wallets" in the protocol.

Wildfire: Arweave also utilizes a data-sharing system called "wildfire" whereby Arweave nodes are ranked based on the speed at which each node responds to requests and accepts data from other nodes in the network. Nodes that fail to quickly share information can be blacklisted from the Arweave network permanently. The design is aimed at incentivizing good behavior amongst nodes in the network.

Blockshadows: Arweave implements another data management system called "blockshadows" – a process in which transactions are partially decoupled from blocks in favor of only sending other nodes a minimal block (the shadow) that enables other nodes in the network to re-create the full block. Blockshadows contain a hash of the wallet list, hash list, and a list of transaction hashes from the current block.

Permaweb: Another notable aspect of Arweave's network is the "permaweb" which sits atop of Arweave's data storage layer. The permaweb is the human-readable layer that contains the collection of documents and applications of which the data is stored permanently on the Arweave protocol. Because the Arweave network is built on top of the HTTP protocol, browsers have the ability to access permaweb documents and applications.

3. FQR Weave:

QR codes and anti-counterfeit:

QR codes are widely adopted primarily because they are extremely cheap, and because of their visual aspect they give the feeling of something cryptic, hence secure. The production cost of a single code is basically zero, which may be one reason brands keep on adopting it even today. The problem being that the reproduction cost of such a code is also zero. When using 2D codes based on standards (ISO/IEC 18004), anyone can create the exact same codes and associate them with fake or counterfeited products, or generate codes that follow the exact same content logic as yours. The replicated or fake code can lead the consumer to a fake website, or just replay real identities leading to the original company systems.

What authentication needs to be based on?

Any product's authentication needs to be based on**:**

- An open standards, which will ease transitions in case of service providers' business failures, avoid vendor lockups and facilitate wider market adoption.
- A security by "open design", meaning the security does not rely on it being secret and hidden, but instead designed from the ground up to be secure and based on code and methods that are in front of enough people.
- Protecting customers and consumers at an individual level, preventing even one single product identity replay scenario.
- The most minimal need for customer or consumer education

Fortunately, using arweave blockchain technology, fQR Weave as a platform will be able to achieve new higher level of anti-counterfeiting and product's authentication solutions.

What is fQR Weave?

fQR Weave is Blockchain-as-a-Service ("BaaS") platform built on the top of Arweave blockchain. The platform in its alpha release will be offering diverse services including: data certificationand documents authentication. With fQR Weave, any sized business, no matter how large or small, can utilize blockchain technology to further enhance brand perception and value as well as to expand into new business models using immutable data.

fQR Weave in its first release will provide only software solution under the form of fQRs. Platform's development will not stop and we aim to be provide a fully functional blockchain based solution by combining software and hardware.

Problems:

The trade of fake merchandise has slowly risen over the last few years and now accounts for 3.3% of global trade, according to a recent report by the Organization for Economic Cooperation and Development (OECD).

Some brands have gone to extreme lengths in an attempt to halt sales of counterfeit versions of their products.

On the other hand, most of times the consumers are victims of counterfeiting. Taking a real life example: a customer in a supermarket might be a victim of a faked expiry date, buying free offers, buying forged products, etc…

Solution:

fQR Weave codes help the anti-counterfeiting process basing on the following blockchain based advantages:

- **Immutability** — the open ledger ensures the records cannot be altered and the owner of each authenticated product can be verified
- **Legitimacy** — fQR codes cannot be forged, as scanning a forged code will reveal the fact of counterfeit at once
- **Validity** — due to the blockchain architecture, the system is able to highlight the status of each item, whether it is "verified", or "invalid TX ID"
- **Transparency** — fQR codes are broadcasted in a public distributed decentralized storage system (blockweave). There is no shady-box in the creation process neither scanning. The operation is done on-chain

Fingerprint QR:

"fQR" in "fQR Weave" stands for **F**ingerprint **Q**uick **R**esponse Code. fQR represents the better version of the standard QR code, for that reason it has been called QR 2.0 .

Each fQR code represents a data TX ID (SHA-256 hash of the Signature). The unique transaction ID is encoded into a QR code which results creating what is called fQR code.

QR code Model 2 is used in the encode process (Fig. 1). It can encode up to 7,089 numerals with its maximum version being 40 (177 x 177 modules).

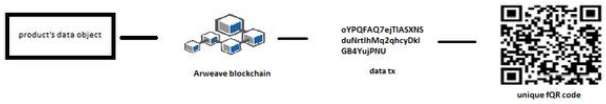

Figure 1: fQR Weave Code generating process

QR Codes also include some error correction information which is some redundant data that will help a QR reader accurately read the code even if part of it is unreadable. There are four levels of error correction: L, M, Q, H. The lowest is level L which allows the code to be read even if 7% of it is unreadable. The another level is M which provides 15%, then level Q which provides 25% and then level H which provides 30% error correction.

The word 'QR Code' is registered trademark of [DENSO WAVE INCORPORATED]

4. fQR Weave Generator:

Overview:

fQR Weave Generator is the tool representing a user interface to interact with Arweave blockchain in intention of creating ownership verified QR codes.

After reaching an agreement with a third-party interested into product's authentication, fQR Weave team develop a custom Generator instance for the third-party to broadcast customized data in the blockweave.

fQR generating process:

The steps for the proposed method are as follows (document -certificate- authentication example, See Fig. 2):

- Compose the message M from the details such as name of the student, father's name, enrollment number, issue date etc.
- Obtain the TX ID value (message digest) of the composed message M, using arweave.js after posting it (broadcasting) in the blockweave
- The University (any academic department) use its Private Key to sign the obtained message digest which will result to a digital signature on message M.
- The data TX ID representing message M is fed into the QR Code generator.
- The QR Code generator produces a QR Code which stores the TX ID.
- The resulting QR code can be printed on the certificate.

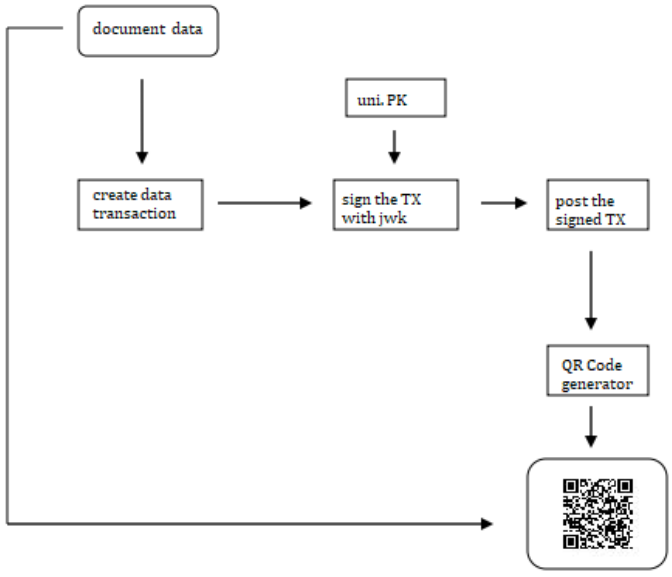

Figure 2: fQR generation workflow

QR code data content is *text/html* hashed in a data TX. This content type is used to broadcast much possible organized information in a single page.

Used arweave blockchain keywords:

ID: SHA-256 hash of the Signature.

Data: Between 0 and 10,485,760 bytes of arbitrary data

Owner: The public key of the RSA key-pair signing this transaction

Signature: The RSA-SHA256 signature of Signature Data Segment for the RSA key-pair where the public key is Owner.

5. fQR Weave Reader:

Overview:

fQR Weave Reader (scanner) is where end-user (consumer) interact with arweave blockchain indirectly. The main point of fQR Weave is the simplicity in integrating web3.0 and blockchain technologies in people daily life. Whether being a person with a programming background, or a non-code person with zero knowledge about blockchain, both are able to use fQR Weave with ease benefiting from Arweave.

fQR Weave Generator and fQR Weave Reader are uploaded into the blockweave to ensure fQR Weave platform strength for being: zero-backend platform (running in user's browser), on-chain, accessible permanently, zero point of failure, and immutable HTML pages to ensure its security against exploits.

Procedure to check product's authentication by using fQR Weave Reader:

- The information in the QR Code consists of TX ID generated by "owner" verified address
- End-user opens fQR Weave Reader and scan a printed QR code
- fQR Weave Reader able to scan and decode any QR code data (additional flexibility). If it's a TX ID, the user needs to interact with arweave blockchain.
- The TX ID string (43 char) is pasted in the "search" field
- On user's click, the reader check the signer of the searched TX ID, if the "owner" exist in the verified owners array, the reader redirect the user to product's HTML data page: *https://arweave.net/TX_ID*
- If the owner is not present in the verified owners array, an alert pop up

Verified Wallets Array:

Because fQR Weave Reader is broadcasted in the blockweave, hence it's immutable and there is a consistence need to keep it like it is –immutable- with the ability of being up-to-date to a list (array) of new comers into fQR Weave arena.

To bypass the obstacle of publishing new fQR Weave Reader version after each user addition, the reader use Last_TX method provided bt arweave.js to read the last TX broadcasted by fQR Weave Verfication wallet.

Each transaction signed by fQR Weave Verfication Wallet consist of an array containing a single item of string type representing verified public keys of the RSA key-pair. (or "n" is the JWK json keyfile).

Last Transaction: The ID of the last mined transaction created by a wallet

Factors which determine the readability of QR Code:

There are certain factors which determine the readability of QR Code (applicable with fQR case):

Size/Distance: The size of the QR Code and the distance of scanning it determines whether it is readable or not.

Modules: The more information QR Code contains the denser it will be and that will make reading it more difficult.

Lens Quality of a Smartphone: The smartphone with macros (ability to focus up close) can read the small QR Codes whereas smartphone with poor camera quality finds difficult to read them.

Light: QR Code may be unreadable in low light or in a backlight surface.

Angle: "There is a tolerance of skewed catch the QR form 20-30° vertically or horizontally"

6. Profit Sharing Community:

Overview:

Profit sharing communities (PSCs) are a new, fairer structure for web startups made possible by the unique affordances of the Arweave protocol. These communities give founders more control and flexibility over their projects, while granting contributors to those projects more power.

Profit sharing communities go a step further in providing sustainable economics for apps,

integrating a decentralized autonomous organization (DAO) governance structure with profit sharing token technology.

What Are Profit Sharing Tokens?

Profit Sharing Tokens (PSTs) are a novel way of incentivizing and rewarding both permaweb app founders and external contributors to a project.

fQR Weave PSC:

fQR Weave PSC information:

- Token Ticker: FQR
- Initial Total Supply: 100,000,000 FQR
- SmartWeave ID: l4iqeiSb4oJrpByg6rgiXlW1iF3cgjXLbHdG2JvAC_c
- Quorum: 50%
- Support: 50%
- Vote Length: 2000 blocks (~3 days)
- Lock min/max length: 720 blocks (~1 day)

Business Model:

fQR Weave PSC business model is different than most of other Arweave PSC, and that's due project's business field.

Platform main users are business owners (retailers, foods, legal documents…), for that reason FQR holders will receive their dividends in a different distribution method.

About 90% of arweave PSC integrated apps reward their holders from application's users interactions (e.g charging fees for uploading a post on a social arweave network). In the other side, for expanding and adoption matters, fQR Weave don't charge fees for generating a fQR or scanning it.

Hence, we have decided to distribute dividends in the form of AR tokens for FQR holders from fQR Weave Generator subscription fees.

Dividends Distribution:

After making an agreement with a client for using fQR Weave as a service, they have to pay monthly subscription fee which covers technical support, generator instance improvements and any kind of fQR Weave related support.

At the end of each month, we distribute 50% of total collected subscription fee as follows:

$$\frac{holder\ FQR\ amount}{total\ holders\ FQR\ \ amount} \times (50\% \times total\ subs\ fees)$$

Subscription Plans:

fQR Weave subscription plans (for generating fQRs) are not decided. After analyzing the fields in depth, we will publish the plans details which will be flexible with the protocol difficulty.

The plan's fee will be paid in AR token by fQR Weave clients. More information regarding this section will be published in the near future.

7. Conclusion

Most of blockchain based apps (or dapps) and platform consider that their users already have knowledge about the web3.0 and blockchain techs. But here, with fQR Weave, we aim to integrate blockchain technology in anyone's life – regardless his background – in a form of anti-counterfeiting platform using well known endcoding model: QR code; and arweave blockchain from the otherside.

fQR Weave simplicity let people more able to adopt and use it.

References:

[1] The Counterfeit Problem And How Retailers Can Fight Back in 2020

https://www.forbes.com/sites/forbestechcouncil/2020/03/17/the-counterfeit-problem-and-how-retailers-can-fight-back-in-2020/?sh=3a93e1a01f32

[2] QR Code Model 1 Model 2

https://www.qrcode.com/en/codes/model12.html

[3] Arweave: Profit Sharing Communities

https://www.arweave.org/profit-sharing-communities

[4] Degree Certificate Authentication using QR Code and Smartphone

https://www.researchgate.net/publication/280291556_Degree_Certificate_Authentication_using_QR_Code_and_Smartphone

[5] QR Code

https://en.wikipedia.org/wiki/QR_code

[6] Arweave Yellow Paper

https://www.arweave.org/yellow-paper.pdf

[7] Profit Sharing Communities: A Deep Dive by Arweave

https://coinmarketcap.com/alexandria/article/profit-sharing-communities-a-deep-dive-by-arweave