GUNCERT: A Peer to Peer Electronic System for the Creation of Tokens, Transfer & Record Keeping of Firearms

James Story
Ryan McDonald
www.guncert.org
12th April 2019

In the scrutinized and high profile world of guns we need smart decentralized solutions to accommodate current regulation, and auditing, for the protection of the sellers, owners, and buyers of firearms, in a way that does not infringe upon their second amendment rights as well as first amendment rights to privacy, we look to blockchain technology to facilitate this effort.

First and foremost, thank you to the vast sea of developers and early adopters that have made blockchain technologies a reality, and continue to use and support them. It is because of your countless hours of work, and dedication that this technology exists and continues to thrive. Without your efforts, none of this would be possible.

Lastly thank you to everyone involved in Ravencoin, as this project is built on that solid foundation. The white paper contained below uses the Ravencoin whitepaper heavily and we are appreciative of the hard work involved in its creation.

Abstract. GUNCERT, is an application layer management platform for a distributed ledger, built using blockchain technology and optimized for transferring assets, and recording those transfers authoritatively in a way that insures record integrity. The need to easily prove ownership while maintaining privacy for gun owners and the need for a gun friendly web hosting and payment platform, in industries that continue to be de-platformed. Key features include cryptocurrency supported payment gateways, web hosting, traditional payment processing, authoritative asset records, real time transfer attestation via the block chain, and immediate update of asset ownership for end users, and regulatory bodies via a decentralized platform. GUNCERT is intended to prioritize security, equal access to commerce, consumer control, privacy, censorship resistance, and asset ownership attestation. It will be quick, easy to use, and allows for easy adoption for technical adopters and every day end users alike.

1. Introduction

A blockchain is a ledger showing the quantity of something controlled by a user. It enables one to transfer control of that digital representation to someone else. Of the many possible uses for blockchain technology, the reporting of who owns what is one of its core functions. This is likely why the first, and to date most successful, use case for blockchain technology has been Bitcoin, which was announced by Satoshi Nakamoto on October 31, 2008[1].

Tokenized assets can be used for a wide variety of purposes, and Tokens offer several advantages to traditional shares or other participation mechanisms, e.g. faster transfer speed,

increased user control and censorship resistance, and a reduction or elimination of the need for a trusted third party by Tron Black and Bruce Fenton 3rd April 2018[2].

GUNCERT will focus on the utilization of the Raven protocol as it is "designed to efficiently handle one specific function well: the transfer of assets from one party to another."[2] GUNCERT will rely on the Raven protocol which provides a use case focused blockchain that provides advantages for this specific use case -- the firearm industry.

One of GUNCERTs goals is to make transfer of firearm assets, and the tracking of those assets increasingly frictionless for American citizens, businesses, law enforcement and regulatory bodies alike. Additionally, we aim to allow easier communication from those same parties based on the use of tags, and messaging, for situations such as, but not limited to, product recalls. As the country continues to see growing divide over gun control laws, and ownership, and as law enforcement and regulatory bodies continue to face issues with tracking and auditing gun ownership and asset records in an authoritative way, GUNCERT provides a common-sense solution. It will simplify the burden placed on individual owners performing independent 3rd party transactions by using tags and tokens to verify the assets involved and serving as verification that the buyer and seller have been vetted. It will simplify the process of maintaining records for firearms and other serialized NFA items for law enforcement and businesses, while significantly decreasing the time it takes for both of those parties to have updated verified records, and it will allow for maintenance and usage record keeping for collectors and enthusiasts in a way that facilitates those records being transferred with the firearm at time of sale via Interplanetary File System (IPFS).

2. Law Enforcement, and Regulatory Bodies

Currently there is no software that allows for quick trace and follow up for displacement of a firearm for law enforcement. Additionally, there is no current integration between businesses and law enforcement agencies for digitally uploading transfer records at time of sale. The current system for businesses and government agencies is slow and dated, and easily subject to fraud and error.

When purchasing a firearm from a licensed gun dealer, a buyer must fill out form ATF 4473, which includes the same basic information they would need to be issued a government ID. [3] This system relies on that dealer calling a local agency for processing a low-level background check, with records that may or may not be up-to-date. There is no centralization of the data used to verify this buyer's ability to legally purchase and own a firearm. While this is available to individuals selling their firearms in third party transactions, it is not easy to do and is not required.

Additionally, if the ATF or law enforcement needs to determine transfer of a firearm, it requires the ATF contact the manufacturer who originally sold the gun to begin the trace. GUNCERT can solve both of these problems by allowing law enforcement to track the movement of an asset on the blockchain whether that transfer was conducted by a licensed gun dealer, or by a third-party owner, and allows third party unlicensed sellers to quickly verify the person they are selling the firearm to can legally purchase a firearm. Because this can be done without needing the owners

identifying information, it is only a means to identify transfers, and not the parties being transferred to and does not act as a national registry, or risk disclosing the identity of the end owner. This is important for privacy, and because a national firearm registry is illegal.

Examples:
1. A user creates a GUNCERT profile, at that time they provide their concealed weapons permit, and basic form 4473 information, or pay for a background check. After verifying the person's identity, and ability to lawfully own and purchase firearms, a tag is issued to that persons wallet that is valid for the length of the permit, or permit laws in their state, signifying they have been verified. After verifying the user, GUNCERT destroys the PII linked to the user. Then a second user wanting to sell the first user a firearm now has the ability to verify they are selling to a legal gun owner without the buyer needing to divulge an excessive amount of personal information.
2. A firearms manufacturer creates a GUNCERT account and is issued a range of tokens for creating firearms with a serial number to asset token match. Those assets are then transferred to a gun store with a GUNCERT account, and those firearms are sold to end users. The transfer of the firearms is propagated across the network after each transition, and allows the ATF to audit inventory, without having access to the information of the end users and owner of the firearm, and without needing to visit the businesses and manually audit their books.

3. Businesses and Gun Owners

Businesses and gun owners stand to benefit from this system as well by easing their ability to make smart, quick transfers, with detailed up-to-date records, and by easing the burden to perform these tasks and maintain legally required records and information about the history and life of the asset being transferred.

Much like a Carfax report, gun owners can keep logs for the use and maintenance of their firearms in IPFS. As such, gun buyers would be able to request such records to verify proper care and maintenance of the firearm, and presence of such records and the asset token corresponding with the firearm being sold would ensure they are buying it from the legal owner of that firearm. This would be especially useful to businesses like pawn shops. After purchase, the record of the firearm would be transferred with the digital asset to the new owner allowing that owner to receive messages associated with that token from the manufacturer, and to verify they own that asset. It has B2B applications as well by allowing businesses to track inventory, shipping, time of receipt, in a way that allows all parties to verify when and how assets are received and disposed of without the risk of records being falsified or relying on third party verifiers.

4.Full Asset Aware Protocol Level System

Ravencoin is a bitcoin-like system that is fully asset aware, which provides two major advantages. First, it allows the client and RPC commands to protect the asset from being destroyed accidentally. Second, it allows a single native client to issue, track, and transfer the assets. Lastly, to provide security for the underlying assets, the system functions only with a market value, regulatory enforcement, and wide distribution.

Assets

Assets are tokens that can be issued by users of the Ravencoin protocol without the need to be mined. Users of the Ravencoin protocol create these assets and decide their purpose and rules independent of the protocol. For use with GUNCERT, these rules and purposes will be defined and maintained via the application layer of the software. These assets or tokens exist on the Ravencoin blockchain and could be whatever name, denomination or purpose selected by the creators of each asset, coin, or token. For this use case, tokes will correspond to serial number for firearms and other NFA items. The tokens are transferable and move with the same ease as bitcoin, or other similarly functioning cryptocurrencies. In Ravencoin, an asset is just a limited quantity of a unique symbol, and transferable to any Ravencoin address. Assets created on the Ravencoin protocol have several advantages: they are easier to use, tightly integrated with a native coin, and secured with fair POW mining and open source code not run by a centralized organization as described by Tron Black and Bruce Fenton 3rd April 2018[2].

Uses for Assets

Like traditional fiat systems, Assets or tokens are used stand-ins backed by real world items.

Representing real world custody of physical or digital assets to tokens

- Firearms
- Suppressors
- Ammunition
- Explosives
- Other NFA items

5. Asset Issuance & Transfer

Token names are guaranteed unique. The first to issue a token with a given name is the owner of that token project by Tron Black and Bruce Fenton 3rd April 2018[2]. This allows firearm manufacturers to create schema for tokenization that correlate to the make, model and serial number of assets at time of production.

Asset creation with Ravencoin, allows for a fine level of granularity including options for number of issued assets, whether they are re-issuable and more. This provides adopters of the technology flexibility in implementation, and many potential use cases.

Assets will all facilitate the use for Point of Sale (POS) systems, inventory tracking, Enterprise Resource Planning (ERP), and recall or other assets owner communications. Businesses, gun owners and manufacturers can "easily issue new assets, report current balances, and transfer to other users" according to Tron Black and Bruce Fenton 3rd April 2018[2].

This project allows for control to be vested in the using parties, and does away with need for oversight or potential risk of abuse from "bosses, rulers, employees and corporate structures" according to Tron Black and Bruce Fenton 3rd April 2018[2]. It provides a means to watch the watchers so to speak, by eliminating the risk of government censorship or abuse by editing, destruction, or loss of records. It gives gun owners, and businesses a way to dispute or verify assets transfer and ownership with records that are immutable, and decentralized.

6. Unique Tokens described by Tron Black and Bruce Fenton 3rd April 2018[2]

Unique tokens allow token holders to create unique assets. Like ERC721 tokens, unique tokens are guaranteed to be unique and only one will exist. Unique tokens can change ownership by sending the unique token to another user's address.

Some examples of unique tokens:

- Imagine an art dealer issues the asset named ART. The dealer can then make unique ART assets by attaching a name or a serialized number to each piece of art. These unique tokens can be transferred to the new owner along with the artwork as a proof of authenticity. The tokens ART#MonaLisa and ART#VenusDeMilo are not fungible and represent distinct pieces of art.
- A software developer can issue the asset with the name of their software ABCGAME, and then assign each ABCGAME token a unique id or license key. The game tokens could be transferred as the license transfers. Each token ABCGAME#398222 and ABCGAME#423655 are unique tokens.
- In game assets. A game ZYX_GAME could create unique limited edition in-game assets that are owned and used by the game player. Example: ZYX_GAME#SwordOfTruth005 and ZYX_GAME#HammerOfThor These in game assets could then be kept, traded with other players via QR codes and wallets or uploaded into an upgrade or different version of a game.
- RVN based unique assets can be tied to real world assets. Create an asset named GOLDVAULT. Each gold coin or gold bar in a vault can be serialized and audited. Associated unique assets GOLDVAULT#444322 and GOLDVAULT#555994 can be created to represent the specific assets in the physical gold vault. The public nature of the chain allows for full transparency.

Example:

The holder of the token GUN could issue a unique token for each firearm by including the serial number.

Example: GUN#W1102658

Some use cases for unique assets include:
- Firearms
- Suppressors
- Ammunition

- Explosives
- Other NFA items

7. Payment Processing and Web Hosting

The modern tech world has shown itself to be a very unfriendly landscape for the firearm industry. Stripe, Paypal, Mula, Authorize.net, Volusion, Shopify, Pinterest, Reddit, Instagram, Twitter, Facebook, and Google all have implicitly biased policies that limit the way or completely prohibit firearm related business from using their platforms. These companies are not unique in this regard, and every year we see the footprint of businesses that are antagonistic to the gun industry, yet it continues to grow.

GUNCERT will allow for payment processing, via conventional means, and cryptocurrency, and will provide ecommerce hosting solution for gun related businesses. Guncert will also support B2B advertising and content sharing similarly to social media platforms and Google Adsense by allowing businesses to both advertise their products, and monetize their websites by providing ad space to in network companies.

8. Privacy described by Tron Black and Bruce Fenton 3rd April 2018[2]

It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations. (Wei Dai)

Privacy is key in investments and tokens because financial systems function better when assets are fungible and can trade in a frictionless manner. The project should seek to strengthen privacy in any way possible as future technological improvements are made, while still allowing accurate tracking of firearm ownership.

As capabilities like messaging, assets, and rewards are added, privacy will be preserved in the same way that UTXO based cryptocurrencies separate identity from public addresses. "Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient.

When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself. "Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy." (E. Hughes) [5].

9. Other Projects Can Use This Platform

We intend for this system to be transparent, and compatible with third party integrations by allowing all Non Personally Identifiable Information (PII) data to be accessible by API.

10. Conclusion

Gun control is a subject of much debate, and the firearm industry is continually on the losing side of that debate. Modern e-commerce providers, and payment providers continue to de-platform and not allow the gun industry to take advantage of critical business services, and the need for modern solutions to these problems is extremely high. GUNCERT can provide the systems to ensure Americans are able to safely and fully embrace their second amendment rights with a solution that is feature rich for gun owners, dealers, manufacturers and government agencies.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf
[2] B. Fenton, T. Black "**Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets**" https://ravencoin.org/assets/documents/Ravencoin.pdf
[3] https://www.npr.org/2013/04/11/176954637/gun-registration-paper-trail-is-long-and-convoluted
[4] W. Dei, "B-Money" http://www.weidai.com/bmoney.txt
[5] E. Hughes https://www.activism.net/cypherpunk/manifesto.html

Not directly cited but directive of citations from the Ravencoin whitepaper and other works:
[1] https://en.bitcoin.it/wiki/Colored_Coins
[2] https://en.bitcoin.it/wiki/OP_RETURN
[3] https://bitcoinwisdom.com/bitcoin/difficulty
[4] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[5] https://github.com/Dexaran/ERC223-token-standard
[6] https://www.ethereum.org/
[7] B. Fenton, "Ravencoin: A digital peer to peer network for the facilitation of asset transfers." https://medium.com/@ravencoin/ravencoin-4683cd00f83c
[8] https://github.com/RavenProject/Ravencoin
[9] T. Black, J. Weight "X16R" Algorithm White Paper
https://ravencoin.org/wpcontent/uploads/2018/03/X16R-Whitepaper.pdf
[10] http://coinspark.org/developers/assets-introduction/
[11] N. Szabo, "Secure Property Titles with Owner Authority"
http://nakamotoinstitute.org/secure-propertytitles/#selection-7.7-7.50
[12] https://www.forbes.com/2008/09/23/naked-shorting-trades-opedcx_pb_0923byrne.html#63076e102e6c
[13] https://en.wikipedia.org/wiki/Delegative_democracy
[14] https://bitcoin.org/en/glossary/unspent-transaction-output