Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets

Bruce Fenton
Tron Black
www.ravencoin.org
3rd April 2018

In the fictional world of Westeros, ravens are used as messengers who carry statements of truth. Ravencoin is a use-case focused blockchain designed to carry statements of truth about who owns what assets.

Thank you to the Bitcoin founder and developers. The Ravencoin project was launched based on the hard work and continuous effort of over 430 Bitcoin developers who made over 14,000 commits by the date of the Ravencoin code fork. We are eternally grateful to you for your diligence in making a secure network and for your support of free and open source software development. The Ravencoin project is built on the foundation you built.

Abstract. Ravencoin is a blockchain and platform optimized for transferring assets, such as tokens, from one holder to another. Based on the extensive development and testing of the UTXO model of the Bitcoin protocol, Ravencoin is built on a fork of the Bitcoin code. Key changes include a block reward time of one minute, a change in the number of coins issued, but not the weighted distribution schedule and the addition of asset creation and messaging capabilities. Ravencoin is free and open source. All Ravencoin (RVN) are fairly issued and mined publicly and transparently using Proof of Work (POW) using the x16r algorithm which was created for Ravencoin. There is no private, public, founder, or developer allocation set aside. Ravencoin is intended to prioritize security, user control, privacy, and censorship resistance. It is open to use and development in any jurisdiction, while allowing simple additional features for users based on need.

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].

The Ethereum ERC20 protocol and other projects show tokenized assets that use another blockchain can be created with a wide variety of purposes and structures. 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.

Bitcoin also has the capability of serving as the rails for tokens by using projects like Omnilayer, RSK, or Counterparty. However, neither Bitcoin nor Ethereum were specifically designed for facilitating ownership of additional assets, and the users and development teams generally prioritize other features.

Ravencoin is designed to efficiently handle one specific function well: the transfer of assets from one party to another. One goal of the Raven protocol is to create a *use case focused blockchain* and development effort which can create code, providing advantages for specific use cases, while contributing to open source code which could be used by Bitcoin or other projects.

If the global economy is influenced by actors using various blockchains, then the way capital markets work today could also change. Borders and jurisdictions may become less relevant as more assets become tradable and trading across borders grows increasingly frictionless. In an age where people can move significant amounts of wealth instantly using Bitcoin, global consumers will likely demand the same efficiency for their securities and similar asset holdings.

2. Background Tokens and Other Assets

On January 3, 2009, Bitcoin was launched as a *peer-to-peer electronic cash system*. Years later, after it achieved a notable level of security, it was recognized that assets could be created "on top of" or embedded in the Bitcoin blockchain. New assets can be added to the Bitcoin blockchain by creating secure, signed, immutable bitcoin transactions which also carry information on asset issuance, and transfer.

There were several projects that added tokens to the Bitcoin blockchain. The first was Mastercoin [2] by JR Willett, followed by Counterparty [3] and other projects. One category of protocols developed to facilitate the creation of assets on the Bitcoin blockchain became known as Colored Coins [4], as they mark bitcoin transactions with specially crafted transactions in the OP_RETURN [5], which is like a comment field in the Bitcoin protocol.

The advantage of embedding assets in the Bitcoin blockchain is the high level of security. Bitcoin is considered by many to be the most secure blockchain because there is a tremendous amount of distributed mining power that secures each block with a "high difficulty hash"[6]. Because the distributed Bitcoin nodes recognize the level of effort to create a high difficulty hash, this makes it nearly impossible to re-write, or modify the blockchain without prohibitively high mining investment. To tamper with the Bitcoin blockchain, to re-write or modify its ledger, would take significant efforts from an investor at the level of a nation state.

The disadvantage of embedding assets in the Bitcoin blockchain is that the Bitcoin rules must be followed as originally written, and the Bitcoin nodes are unaware that assets are being embedded. This means that a Bitcoin transaction must be used for every asset transaction, and it must send enough bitcoin to be considered a valid transaction, even though the primary purpose of the transaction is to send the asset. That is inconvenient, but a major disadvantage is that a Bitcoin client that spends that bitcoin without being aware of the embedded asset transaction will destroy the asset. For example, a holder of the Bitcoin private keys to Bitcoin which hold the Counterparty assets, could accidentally send that Bitcoin to an exchange or wallet and lose those assets. A partial solution to solving this issue is to create a special address format that is used for the asset, but that doesn't prevent the mistake that may destroy the asset. It just provides more clues that there is an asset embedded in the transaction.

Other token standards like ERC20, ERC721 and ERC223 are built on Ethereum or other blockchains that support smart contracts. A different problem exists when using these smart contracts. Since the Ethereum network does not natively recognize these smart contract tokens, it is currently unable to protect against some common problems. Smart contracts can be confusing for users as there can be multiple ERC20 tokens with identical names. The only distinction between contracts with identical names is the contract hash.

3. Full Asset Aware Protocol Level System

Who will not change a raven for a dove? The will of man is by his reason swayed. – William Shakespeare

The solution is to create a bitcoin-like system that is fully asset aware. A system being asset aware 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 bitcoin-like system functions only with a market value, a strong mining community, and wide distribution.

Assets
Assets are tokens that can be issued by users of the Raven protocol without the need to be mined. Users of the Raven protocol create these assets and decide their purpose and rules independent of the protocol. 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. 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 have been available for some time on other platforms such as Open Assets, Mastercoin, Counterparty, and as an ERC20[7] or ERC223 [8] token on Ethereum [9]. Assets created on the Raven 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.

Uses for Assets
Assets or tokens can be used for anything the creator's imagination can conjure. The ideas presented here are a sampling.

Representing real world custodied physical or digital assets to tokens

- Gold bars
- Silver coins
- Physical Euros
- Land Deeds
- DC Comics Presents #26
- Energy credits (Electricity, Wood, Gas, Oil, Wind)

Representing a share of a project

- **Securities tokens:** stock or shares of a company where the shares are represented by a token rather than a physical stock certificate
- Securities or partnership interests with the built-in ability to pay dividends in RVN (legal in many free market countries)
- Tokens which represent a coop, limited partnership, royalty sharing or profit sharing platform
- A token which represents a crowd-funded item with the ability to transfer or resell the item

Representing virtual goods

- Tickets to an event such as a Baltimore Ravens game with the ability to resell
- A license to allow an activity
- An access token to use a service
- In-game currency and items, transferable outside of the game platform

Representing a credit

- Gift cards
- Airline miles
- Reward points

Satoshi Nakamoto described bitcoin as an implementation of Wei Dai's bmoney [10], designed to afford users more control, security, and privacy than more centralized systems. A design with the potential to prevent violence and discrimination, given the holder of bitcoin remains private. Ravencoin aims to continue this implementation by focusing on assets other than cash, providing a

platform that users can easily issue assets they control under the rules they establish on a secure blockchain.

4. Ravencoin Launch and Algorithm

Ravencoin was announced on October 31, 2017 [11] and released binaries for mining on Jan 3, 2018, [12] the respective ninth anniversary of the announcement and launch of Bitcoin. Ravencoin is the bitcoin-like system that will allow users to issue and integrate assets into its blockchain. This will be accomplished in phases which build upon each other.

- In progress

Create a platform like Bitcoin with a new mining algorithm, x16r [13], intended to prevent immediate dominance by mining pools, and future dominance by ASIC mining equipment.

Launch the token with no pre-mine and a fair launch to widely distribute the tokens.

Allow the mining rate to increase and the value of the RVN token to naturally grow and gradually disburse to holders that understand the value of the platform.

Utilize proof of work mining, not because it burns a scarce resource of electricity, or the requirement of computer hardware, but instead focuses on the most valuable part of the "work" which is building an ever-larger and time-based wall that protects user data from future tampering and censorship with every new layer.

5. Asset Issuance & Transfer

Deep into that darkness peering, long I stood there wondering, fearing, Doubting,
dreaming dreams no mortal ever dared to dream before;
But the silence was unbroken, and the stillness gave no token.
- Edgar Allen Poe, The Raven

Token names are guaranteed unique. The first to issue a token with a given name is the owner of that token project.

The issuer of a token burns RVN and must provide a unique token name. The issuer determines the quantity issued, the number of decimal places, and whether they will be allowed to issue more of the same token in the future.

Allow the issuance of other tokens using similar method as Mastercoin, Counterparty, or CoinSpark [14].

Tightly integrate assets with the GUI wallet and create new RPC calls, which provides intuitive asset management. Easily issue new assets, report current balances, and transfer to other users.

The combination of open source and the shared incentive mechanisms enabled by blockchain based tokens enables interests to be aligned in ways that traditional structures cannot.

Fair and open source token projects can replace bosses, rulers, employees and corporate structure with aligned interests & economic choice for participants.

So, in some cases, whether one is selflessly, or selfishly motivated, open source may be a better model for many new and interesting types of projects than other structures. Ravencoin will allow projects to issue tokens to represent co-ops, corporations or partnerships.

Co-ops, for example, are a common organization form in which employees and participants are owners. Large organizations such as Credit Agricole, REI, Land O' Lakes, Ace Hardware, Co-op Kobe, Sunkist and Ocean Spray are structured as co-ops. Despite offering many advantages to participants, co-ops are sometimes difficult to structure and maintain. Tokenizing co-op interests opens many new ways this structure can be used to allocate resources and capital. Since the rules for each token can be changed by each issuer and the record keeping is done on the Ravencoin blockchain with the work distributed, organizations can adapt and deploy a variety of participation structures.

In addition, since the tokens can be made either unique, limited, or fungible by the issuer, token project managers will be able to have categories of token holders such as “Class A Shareholders”, “Lifetime social club members”, “Benefactors”, or “Holders of __ in game item”.

Tokens allow easier issuance of small scale public offerings.

“In the future the size distribution of multinationals will approach that of local business. The phase change between these states may be quite rapid as telecom and transport costs pass through a "melting point", creating a wide variety of new multinational small businesses, and industries to support those businesses.” Nick Szabo, Secure Property Titles with Owner Authority, 1998[15].

This also could decrease fraud, Economist Dr. Robert Shapiro noted significant evidence of Wall St. fraud which can be tied to custody issues (Patrick Byrne, PhD [16]).

Only an open protocol will work in a global economy where there are multiple jurisdictions, each with complex and conflicting regulations.

6. Rewards

Allow the payment of rewards (or dividends) in the native token. With a single command the reward, denominated in RVN, is automatically divided evenly and sent pro-rata to the holders of the asset.

Example:

A young child, in a country that permits it, could create a token that represents a lemonade stand business. Suppose she creates 10,000 LEMONADE tokens. These tokens could be used to raise funds for the lemonade stand at AUD$0.01 per LEMONADE token allowing her to raise AUD$100 to build her business. These tokens can be sold and transferred easily by the owners. Suppose the lemonade stand does extraordinarily well because the neighborhood is invested in this entrepreneurial project. Now our fictional eight-year-old wants to reward those who believed in her project. With one command, she can send profits - denominated in any value RVN may have - to LEMONADE token holders. There could even be new holders of LEMONADE tokens that she's never met. The built-in ease of use should allow anyone, anywhere in the world to do so on a mobile phone, or computer running Windows, Mac, or Linux.

For such a global system to work it will need to be independent of regulatory jurisdictions. This is not due to ideological belief, but practicality: if the rails for blockchain asset transfer are not censorship resistant and jurisdiction agnostic, any given jurisdiction may conflict with another. In legacy systems, wealth was generally confined in the jurisdiction of the holder and therefore easy to control based on the policies of that jurisdiction. Because of the global nature of blockchain technology, any protocol level ability to control wealth will potentially place jurisdictions in conflict and will not be able to operate fairly.

7. Unique Tokens

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 CAR could issue a unique token for each car by including the VIN number.

Example: CAR:19UYA31581L000000

Some use cases for unique assets include:

- Software licensing
- Car registration
- Proof of authenticity tokens to transfer along with items that could be counterfeited
- A token that allows communication on a channel (see Messaging)

8. Messaging Stakeholders

"If the Tower of London ravens are lost or fly away, the Crown will fall and Britain with it." - Unknown

A common problem with tokens/assets is that the token issuer cannot communicate with the token holders. This must be handled very carefully because the token holders do not always wish to be identified. The communication should allow the token holder to opt-out at any time. The message system should only allow select parties to use the message channel so that it is not a spam conduit.

The messaging system uses unique tokens to allow communication on the main token channel. For example, the COMPANY token would have a ~COMPANY:Alert token which allows alerts to be sent to all holders of COMPANY.

Newsletters, game developers, non-profits, activist organizations, corporations and other entities will be able to issue tokens for specific users and then message those users but unlike email or other messaging services, the messaging itself will be enabled only for token holders, thereby making the token transferable.

Messaging to token holders by authorized senders will be layered on top of the unique assets. The unique assets will act as a "talking stick" allowing messages to be sent by the channel owner. *The KAAAWWW Protocol* will be published with more information on this separately.

9. Voting

One of the problems, among many, with the existing US financial system is that all the shares are held in street name. In this age of fast communication, this makes holding a vote ridiculously difficult. A public company that issues shares on Nasdaq, as an example, will have to pay a quasi-monopoly company just to get the mailing addresses of their own shareholders at a given point in time. Then, a physical (dead tree) mailing must be sent out to shareholders with information on how to vote along with a proxy voting form.

By using the messaging system, the holders of a token can be notified of the vote, and by automatically issuing a VOTE token to every holder of a token, the vote can be automated from the client or through a web or mobile interface using the protocol built into Ravencoin.

Tokens are created to represent votes. Ravencoin will create an exact number of VOTE tokens and distribute them 1:1 to the token holders. These votes can be sent via the protocol to addresses that tally the votes. Because the voting tokens move the same way as assets, delegation of votes - sometimes known as delegative or liquid democracy [17] - is possible.

10. Privacy

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.

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) [18].

11. Additional

Other projects can use this chain. Second layer solutions, particularly those being built for projects which share the code base of Bitcoin can be built on the Ravencoin project. RSK, the Lightning Network, confidential transactions, and other scalability improvements, etc. to various open source projects could benefit projects built on this platform.

12. Conclusion

Ravencoin is a platform coin built on the UTXO [19] model of Bitcoin. Modifying Bitcoin code to add these capabilities is not practical, but Ravencoin is a platform built from a code fork and issuing newly mined RVN. Ravencoin will be adding assets, rewards, unique assets, messaging, and voting. The Raven protocol’s capabilities will be rolled out in phases which will be done as a planned hard fork upgrade. The code base is designed to allow users and developers to maintain a secure, decentralized, and tamper resistant network.

The Ravencoin project can also serve as a base and starting point for projects, second layer solutions, experiments, and business ideas which might benefit from either the Bitcoin-based code base with adjustments or the native additional features added to the Ravencoin blockchain.

The Inuit, Tlinglit, Tahitian, Chukchi, Sioux, the Haida, and many others call Raven the magical keeper of secrets, the trickster, friend of the First Men and Creator of the World - an idea or force able to shift, change, and create something from nothing. In open source, the power of the crowd can accomplish much more than any one person or organization. All are welcome to contribute.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[2] https://bravenewcoin.com/assets/Whitepapers/2ndBitcoinWhitepaper.pdf
[3] https://counterparty.io/
[4] https://en.bitcoin.it/wiki/Colored_Coins
[5] https://en.bitcoin.it/wiki/OP_RETURN
[6] https://bitcoinwisdom.com/bitcoin/difficulty
[7] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[8] https://github.com/Dexaran/ERC223-token-standard
[9] https://www.ethereum.org/
[10] W. Dei, “B-Money” http://www.weidai.com/bmoney.txt
[11] B. Fenton, “Ravencoin: A digital peer to peer network for the facilitation of asset transfers.” https://medium.com/@ravencoin/ravencoin-4683cd00f83c
[12] https://github.com/RavenProject/Ravencoin
[13] T. Black, J. Weight “X16R” Algorithm White Paper https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf
[14] http://coinspark.org/developers/assets-introduction/
[15] N. Szabo, “Secure Property Titles with Owner Authority” http://nakamotoinstitute.org/secure-property-titles/#selection-7.7-7.50
[16] https://www.forbes.com/2008/09/23/naked-shorting-trades-oped-cx_pb_0923byrne.html#63076e102e6c
[17] https://en.wikipedia.org/wiki/Delegative_democracy
[18] E. Hughes https://www.activism.net/cypherpunk/manifesto.html
[19] https://bitcoin.org/en/glossary/unspent-transaction-output