Florincoin

A scrypt-based coin with an augmented blockchain.

Introduction

Florincoin is a next-generation cryptocurrency with a new feature added to the already powerful blockchain. This open source software was created, with no pre-mine, on June 17th, 2013, by an anonymous member of Bitcointalk.org named skyangel. Florincoin has the scrypt proof of work algorithm and has a 40 second block timer. The technology built upon Florincoin is useful for the crypto world, and on a grander scale, can benefit the internet as a whole.

Florincoin adds the transaction comment feature to the blockchain. This text field can store 528 characters per transaction. Transaction comments are included when sending coins over the network. This can be used simply as a greeting or a thank you note, or on a business level, expressing important details about the transaction. However, the transaction comment capability can be used in more complex ways. For instance, a platform can be built using the text function to store records of payment, such as the hash of a receipt, which will forever be associated with this transaction. It can be a permanent record of receipts for every Bitcoin, Litecoin, and Florincoin transaction. It can also be used to create a perfect freedom of speech application, harnessing hundreds of mining computers as well as wallet clients as a peer to peer network of decentralized free speech nodes.

The tx-comment text feature can also be used to add unique, un-mined coins to the blockchain, which are simply called “color coins”. The color coin protocol will allow users to create any coin they wish, and distribute it using digital signing, in a similar fashion to Bitcoin transactions. However, color coin transactions are more customizable and can be created in user-defined ways. You can create 10,000 color coins to represent 100% stake in a company, or do something totally unique with it. For example, it is possible to issue a color coin upon finding a block starting with the hash “1337”, in which case you’d be awarded some rare “leet coins”.

Proof-of-Existence is something that crypto currency has been used for in the past, and it makes the blockchain valuable as a public notary. In Bitcoin, this is usually done by storing 12 bytes of data in the address field of a transaction. However, Florincoin allows people to make use of the commitcoin protocol without having to resort to measures like destroying Bitcoin or executing complicated M of N transactions that bloat the Blockchain. Proof-of-Existence can be used in a variety of ways, including storing contracts or hashes of contracts in the blockchain for future reference.

Florincoin can also use the tx-comment feature in the blockchain to store a game ladder ranking system. The Florincoin dev team has invented a protocol for playing a turn-based game in the blockchain, which has a many implications for professional gaming as well as professional card game websites. “Provably fair” games can use the Florincoin blockchain to store both the website’s random number hash digest as well as user’s input, which will prove beyond any doubt whether or not the server is cheating the user by changing the numbers.

Currently, Florincoin’s biggest value-add to the world of crypto currency is interfacing the blockchain with the user directly via mobile-friendly web applications. These applications don’t require the user to download any software or even own any Florincoin to make use of the technology.

Color Coin

http://colorcoin.org

http://www.youtube.com/watch?v=uYRJF3gkve4&t=4100

Color coin is a system using Florincoin transaction comments stored in the blockchain. Florincoin users invent these coins by specifying the guidelines of the coins within the text comment. Once they have invented a new coin, it is tradable and trackable in the blockchain. The coin is created simply by signing a message into the blockchain that says something like this: “I am creating a new coin, called BLUE COIN, and I’m creating 100,000 of them!”.

The creator of the coin can designate the purpose, and therefore, the value of the coin. For example, you can create a coin called “ACME Coin” which has a fixed amount of 100,000 that you award to yourself. These

ACME Coins can be used to represent 100% stake in a company, and can be distributed. ACME Coin can then be transferred, just like a Florincoin, on the Florincoin network in a peer-to-peer basis. This means a decentralized Kickstarter is possible with Florincoin. The creator of the coin can either program into his color coin the distribution Using the color coin system as a means to distribute shares to each person who contributes FLO on the network to a specific address, the owner of that address can either program into his color coin the issuance of each share via the transaction paid to him, or he can promise to give color coins to each person who invests in his company. The system can be built upon different layers of implied trust.

Color coin isn't only useful as a way to distribute stock in a company between people. A color coin can be issued as a representation of a bearer bond, which is in general an agreement that any institution makes to repay you with an asset upon receiving this bond. For example, a gold bearer bond can be bought from a vault which entitles you to withdraw 1 ounce of gold from the vault. The bearer bond thereafter has the value of one ounce of gold, or more, depending on how convenient it is to trade that bearer bond rather than trading the physical gold itself. Bearer bonds can be worth less than the gold it is backed by, if the institution that issues the bond is not trustworthy (see: Mt. Gox). With Florincoin, a color coin can be issued to represent a bearer bond. For example, if an owner of a Gold Vault (let's call it "Mt. Gold") decides to issue color coin bearer bonds, they can be sold to users and they will have value so long as the users believe that Mt. Gold will keep their word and continue to allow users to redeem the bearer bonds for physical gold. This would significantly reduce the amount of fraud in the bearer bond market as well as allow bearer bonds to be traded online in a peer to peer basis.

Color coin can also be used to issue rewards points for customers of stores who wish to have fungible coupons. A color coin can be created to be redeemed for a free box of pop-tarts, or a free subscription for a magazine, or whatever the merchant or business owner desires. The idea is to create a market of freely tradable p2p tokens which represent value in the form of a coupon. Currently, trading coupons online must be verified by a trusted 3rd party, but if the color coin protocol were used instead, the 3rd party arbitrators would have no purpose.

Proof-of-Existence / Proof-of-Publication

http://aterna.org/love

It is possible to use Florincoin's blockchain to prove that something has existed at a certain time, within a certain window of time. Florincoin can be used to replace notaries, host contracts in lieu of a lawyer, or to simply prove that something has existed before a certain time.

A perfect example of this is showcased on the website http://aterna.org/love. Here, lovers send each other messages on the blockchain, which are provably sent on a certain time and day. The messages are entered in a form on the website, so the user doesn't have to have any Florincoin to author an eternal love message. The idea is that the blockchain is easily accessible to any person who wishes to use this technology to write anything they want into the blockchain and have it distributed to many mining nodes. The blockchain, as a public ledger stored on many computers, can be accessed by anyone for free and holds all of the information that was input through this webform.

The Florincoin blockchain can be used to store any type of message, not just a love message. For example, someone moving into a new apartment can take photos of the apartment and hash the message into the blockchain before signing the lease. Upon signing the lease, the lease document itself can be hashed and stored into the blockchain, and it will be dated and signed by the landlord and the tenant on paper as well. Any poor conditions or damages in the apartment before the tenant moves in can be photographed, hashed and placed on the blockchain, to prove that the damage existed before the lease was signed.

Proof of Existence is currently being implemented in a few businesses I'm involved in, mainly to store asset ownership titles. The idea of using the blockchain as a historical store of data isn't new, but Florincoin was created for this very purpose as there was no technology that could do it well. Through the power of Florincoin, we've gained an incredible tool to document and record all of history in the blockchain, with the miners incentivized to propagate the data through micropayments on the blockchain.

Gaming in the Blockchain

http://aterna.org/game

http://vimeo.com/87682214#t=45m30s

The gaming video transcription:

"A ranking system for turn based games can be stored on the blockchain. Is anyone familiar with ELO? ELO is a chess rating system, essentially if two people have an ELO rating, using a simple equation you can determine what the probability of beating the other person would be. Technically if you have a really high ELO you are a very good player.

I considered how signatures, cryptology and hashing can be used to prove that you played a game or won a game against another user, and use the protocol to record each turn off-chain, without actually having to store every turn individually on the blockchain. This system would store the beginning of the game, which is everyone agreeing to begin the game, and the end of the game which is the winner posting a hash of the last turn.

The process begins when each user posts a request JSON to the front end. Essentially they provide the transaction message protocol they want to use. They post some information to the front end.

Everyone has to sign a message before the designated block number in order to be playing this game. Eventually after they provide this information, they sign it, and the signature is also posted here.

After you've gathered enough players, or have gathered enough signatures from people that want to play, the game begins. All of that information is put into the blockchain, signaling the start of a game.

Every turn is not stored on the blockchain but it refers to the previous turn hash, and move number, and move code. In chess you move a piece to a certain position, the piece and position combination would be the move code. Every turn is salted, signed and hashed and then used as reference for the next user's turn. Each person's turn is not only hashing their turn but also signing and confirming the previous player's turn, which is also agreeing to the developments in the game.

The front end of this platform would handle all of the technical stuff for most players. A player would be able to see if anyone was cheating or if something weird occurred during the game, especially if they played that game enough, so they would have the option to flag or label that person as a cheater and in this system it would be easy to verify if they made an illegal move.

So each turn contains the data of that turn and confirms the data prior to the turn. At the end of the game, the winner posts the hash of the final turn into the blockchain and is then considered the winner. If any player chooses to dispute the win, the front end of the game would have a system where you can submit the JSON, which is a compilation of every turn that happened and by looking at the signatures and comparing it to the public keys on the blockchain the server would be able to verify that every each move had been confirmed and agreed upon so the game must have been legitimate."

Decentralized Social Network (3 minutes)

Freedom of speech is an extremely important subject, especially now with revolutions taking place worldwide, and governments cracking down harshly on social media. There are countless instances of governments and special interest groups strong-arming ISPs, websites, and social networks like twitter into taking data down from the web that they find unacceptable, even if it is true. Most of the time, it is something inconvenient for them that the public should be aware of, but they will never end up seeing because it is censored. This type of behavior is abusive and backward-thinking, freedom of speech is a basic human right and no government or group should be powerful enough to silence anyone's opinion.

Using Florincoin, freedom of speech is guaranteed by users who wish to have their voices heard. The blockchain can be used to record tweets historically, and unlike the twitter page of a single user, the blockchain can't be erased easily. For the government of Venezuela to take down a tweet from the Florincoin blockchain, they would have to go to each and every user of Florincoin, and tell them to take down their node. The blockchain is a hash result of every block before it, so deleting one message isn't possible. The person would have to give up the entire blockchain to be able to remove the message, or every single user of Florincoin would have to agree to take it down and change the entire blockchain upon the 3rd party's request.

Q&A from the developers

Q: Okay so you are the first with that feature, who cares? Sometimes the first to battle is the first to the slaughter. What differentiates you from the coins that have the same feature?

A: We have the experience gained from over a year of trial and error using this new blockchain as a database for applications built atop our coin. Additionally, our network effect is currently largest, with many introduced to the idea of "Blockchain 2.0 features" via the capabilities of Florincoin applications.

A: BTC being first to market gives it value. Transaction metadata is the future of BTC. In other words, using the new technology of the Blockchain to store external data is already being explored as the future of Bitcoin's potential, and we are the first to market with this important functionality.

Q: Who is skyangel?

A: He could be Satoshi for all I know.

Q: If its so great, why is the market cap <$200k?

A: We can always use some help with marketing. Also, the coin will be in higher demand as new protocols are written and coins must be paid to miners as fees to use the protocol. For example, we're currently working with a company to hash titles into the blockchain and signing them with the user's private key. This not only goes to show that the blockchain can be used in a practical way for legitimate businesses, but at the same time it drives demand for the currency via the payment for the miners doing the work of confirming and storing these transactions.

Q: Considering FLO's forward thinking functionality, why are there not already FLO gaming/gambling sites?

A: The laws in the United States are extremely prohibitive of opening new online gambling and gaming websites. Regulations are tight and mostly unclear, having been written years ago for outdated technology. Bitcoin and cryptocurrencies in general are a new frontier that have yet to be conquered by regulators, so our stance right now is to stay away from this. Of course, this doesn't stop anyone else from using Florincoin as a next-generation provably fair gambling backend.

Q: How will you control the legality of what people choose to post on the blockchain?

A: Messages are hex encoded on the blockchain, so holding a string of hex isn't going to endanger you in any way unless you decode it and spread it to others purposefully. If this were the case, literally any data on your computer or on any web site could be thought of as "illegal material", since encoding and decoding ones and zeroes is a matter of individual choice.

Each Florincoin explorer can choose to display whatever information they wish to on their pages. For example, I've got a "filter" feature on my Block Explorer, which is used to remove offensive or otherwise illegal materials from the transaction-comment database. However, I've never had to use it. Some block explorers have taken a more cautious approach, which is to not display transaction-comments at all.

In the end, it's a matter of choice given to the web developer who is using the Florincoin software. If you want to build a completely decentralized free-speech platform using Florincoin, you can leave the messages uncensored and decode them for all of the world to see. If you want to only display messages signed by private keys of people you trust, you can do that as well (Aterna love implements this structure). The fact of the matter is that this type of free speech is for the first time technically possible with the power of the decentralized open ledger known as the blockchain.

Q: When bitcoin implements transactions comments, will florin have any advantage with more characters available to the user?

A: Bitcoin transaction comments are implemented in OP_RETURN, which allows 40 bytes of data storage. 40 bytes of data storage for a Bitcoin transaction is an extremely low amount of data per satoshi, meaning Bitcoin transaction comments will be far more expensive and complicated to implement. For example, it would be difficult to string two Bitcoin transaction comments together to make one larger one, since the identifier to connect two transaction comments would have to be the previous transaction comment (64 characters of hex). Because of this, it would be impossible to reference a previous transaction within a new transaction. External tools would have to be used to ensure transactions were linked together. Furthermore, OP_RETURN marks the transaction as “unspendable”, which means it will be pruned by most nodes. Florincoin transaction comments will live forever as historical points of data, this is the entire point of Florincoin.