Whitepaper

MediaCoin Executive Summary

Mediacoin seeks to change the way we view security and trust. Looking to ensure that developers of content are the beneficiary of their hard work and talent and are not exploited due to the inability of content distributors to properly secure their content. By assisting with the development of MediaCoin into a multitude of projects, released in phases, that will undoubtedly revolutionize the world we live in. At its core, MediaCoin stands for honesty, integrity, and an unwavering dedication to security and innovation.

Table Of Content

2018-01-25

MediaCoin White Paper

2017-12-06 Rough Draft
2018-01-25 Main
(In order to not violate patent applications in progress, some details and descriptions are omitted.)

Market Analysis

It's expected that the streaming video market will grow to $70.05 billion by 2021 from $30.29 in 2016.[1]

Value to Market

Media content and pirating have become intertwined in today's world. Content handlers like spotify, youtube, and soundcloud have consciously chosen to continue operating in a way that does not protect their client's content. It is easily downloaded, and shared in their original form using browser plugins. The technology is here to provide a solution to these artists, and MediaCoin will deploy it.

---

[1] https://www.prnewswire.com/news-releases/video-streaming-market-worth-usd-7005-billion-by-2021---online-video-streaming-has-increased-viewership-60---research-and-markets-300267717.html

Artist Benefits

Artists have long been forced to “partner” with large content handlers who have been negligent with their content, to put it lightly. We understand that content is more than just a file to an artist. Inadequate security, delayed payment without explanation, and unfair licensing are just a few issues that are brought up on a daily basis between artists who feel they have no alternative to turn to.

Artists will sleep soundly when partnered with Mediacoin. Not only will their content be completely secure using our state of the art encryption software and require no registration fee, but also will receive 100% of the revenue from the purchase of their content immediately after payment by the user. To create a fair and honest license partnership, we do not want royalties, we do not want to charge for advertising (In fact, in some circumstance we pay for that ourselves), what we want is a true partnership and collaboration with the artist. Simply put, we want to change the relationship between talent and distribution.

User Benefits

The MediaCoin platform will be a magnet for licensing and commissioning high value and premium quality content that artists aren’t willing to submit on other platforms. Users will directly benefit from: lower costs, portability between devices, and rapidly increased content delivery in their own language. No longer is a user forced to choose between overpaying for the content they enjoy, or committing a crime.

Users need to understand that when content is stolen, not only the artist suffers. A common tactic employed by distributors is referred to as a “piracy tax.” Assuming that some users will take a legitimate route in acquiring the product, they increase the price to account for the illegally obtained content. By forcing all users to legitimately purchase content, we will in turn benefit both users as well as artists by dramatically lowering the cost required to make the artist a fair profit, and not place the full burden on those who are willing to compensate the artist for their work.

Currently, the market’s best offer is a subscription-based payment model, which does not take into account how little they consume. MediaCoin’s pay-per-play system will optimize the user’s budget by only charging for what they do actually consume at a rate decided by the artist. By simply offering a fair alternative, MediaCoin will be far and away the price leader in the ad-free content delivery network.

Internet users in the United States have been subject to Net “Neutrality” which does allow ISP’s to manipulate search engine results and even change the content of published works. Using cryptography we are able to verify and deliver content, checked from multiple sources and unpacked without interference or alteration.

Artist Services

Unfair payment practices and piracy have left artists holding the short end of the stick. We're intending to change that. By providing content security for media creators as well as a way for them to choose their own business model, we offer a more fair and direct way for content producers to be compensated. Creators choose how much they want to sell their content for, as well as how they would like to license it to consumers: pay-per-play or a one-time fee. In addition, content owners have no middle man to reap the benefits of their work.

Content creators dictate their own payment terms while our technology simply enforces access. If a listener only pays for one use of a song, that's all they get. We offer exclusive and non-exclusive content management, commercial licensing partnerships to a worldwide audience, and provide copyright enforcement.

MediaCoin Network

The MediaCoin network will grow in stages, incorporating the features listed below as they are developed:

Distributed App (DApp)

Mediacoin selects between side channel and blockchain for the purposes of speed and functionality during the transfer of tokens. Media decryption keys are delivered to blockchain addresses by browser plugin.

Peer to Peer (P2P)

Data is hosted on: MediaCoin's central servers, or by members who are paid the delivery fee for data.

Multiple devices

Mobile apps are developed (Android and iOS) for viewing encrypted content, as well as sharing and routing purposes.

Mesh network

Every connected device will have the option of sharing, hosting, relaying or requesting data.

Internet-of-things

The interaction between devices within your network.

ISP Services

MediaCoin will use a variety of wireless technologies and license bandwidth to provide mobile and rural internet access.

Encrypted Content Delivery: Most secure content delivery since the record player.

The primary weakness in the Public-Private key infrastructure that permits "Man in the Middle" attacks has fundamentally been client authentication. Weaknesses have been discovered in the implementations and negotiations with the Public Key Infrastructure, but the secure design required both a certified server and client.
While zero knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK) can be used to verify certain kinds of computations, we believe the major advancement offered by the cryptocurrency wallet plugins is client authentication. For the first time in the history of the World Wide Web, users have begun to adopt public keys accessible by web sites. Moreover, these public keys are tied to addresses that can be verified and used as a means of value exchange, through cryptocurrency, blockchain and even more relevant, tokens within a blockchain. Tokens are an ideal mixture of trust in a trust-less system and internal accounting specific to a particular data silo.

The implementation of user wallets prompts for payment, verifies the transaction with the client, and can be submitted blockchain that will prevent double-spending. Within a data silo, micro-transactions can be performed and tracked with regular bulk submission upon externality referencing events. Properly triggered, the double spend is still prevented and transactional costs can be aggregated and minimized in the same manner as ACH within the banking networks.

Our MediaCoin Token will leverage several advances in infrastructure, user adoption of public key cryptography in wallets, a network token representing value, military grade encryption decryption in secure browser sandboxes, GPU acceleration of memory intensive encryption, protocol enhancements to data tunneling (TOR), peer discovery (DHT) and file delivery (IPFS).

While true privacy is not the goal of our implementation, we will facilitate enhanced privacy by full packet encapsulation in client. Tunneling is a mechanism necessary to content delivery and network access, but our design implementation won't directly increase latency to enhance privacy.

Network Value

In the past, it wasn't feasible to securely deliver content for playback. This insecurity led to user accessing a URL and making unlimited copies of the content. Not only does this violate copyright infringement law, it also deprives the artist the opportunity to monetize their work. The Mediacoin platform has adapted the security model to ensure encrypted files are delivered efficiently and decryption keys are sold into a secure sandbox.

Within the framework of our encrypted delivery system, our media formats are focused primarily upon video and audio playback. We will continue to pursue additional streaming content with a potential entrance into the client software market. To enhance the service we provide, all MediaCoin content will be catalogued, reviewed for proper copyright licensing, sampled for quality and ultimately encrypted. As the process is automated over time as a result of the initial editors of the content verifying it, the uploaders of the content (who will be referred to as the "artists") will choose the price of their content and ensure proper usage rights (examples would be a charge per play or per session.) A per session song on repeat loop would be charged only once and 100% of the price selected by the Artist will be paid. (However, a minimum of 10% will be paid as referrals to the playlist creator, artist referral, user referral, and user referral referrer.) As we scale larger and artists want to sign directly with us, we will offer the commercial license as a direct sale and provide copyright protected services utilizing our proprietary

technology. A per file fee will be assessed, in addition to the artist fee, based on the size of the file and the delivery costs if necessary. Please note that a "per-play" license with the file saved in browser cache will not be charged a delivery fee for repeat play, but will be charged a license for each play.

A revolutionary approach we are bringing to the music and media industry as we monetize MediaCoin is utilizing "tokens" as the traded current of value. Tokens are representations of value, and can be purchased or sold for cryptocurrency and major currencies. The business model for Mediacoin is built around providing 100% artists payout with $0 artist fees using cryptocurrency. To summarize, a user would sign up for a Cryptocurrency Exchange, providing personal identification equivalent to opening a bank account, purchase Ethereum (ETH) or Ethereum Class (ETC), withdraw funds to a Wallet and finally interact with a Smart Contract to receive Tokens. On our website, will charge a premium for buying and selling our Tokens directly to users. The rate will be based on the Exchange rate, with approximately 20% increase above the Market Rate on Exchange to purchase, and 10% below Market Rate to withdraw Tokens as currency.

Freemium

A user of MediaCoin will have the opportunity to opt-in to earn token without payments. Each network, song, playlist, and artist, and commercial license referral will be the primary methods we advocate. In addition, to provide additional revenue streams and continue to expand our operations, we will support an opt-in advertisement view, including incentivized behavior (such as mobile phone app installations and game playing). The tokens that are earned in these ways will not be segregated but will form the foundation of a freemium consumption model. Adblocker rewrite rules installed as a browser extension with limited insertion and a hidden earn-per-click model will be Freemium with minor development. Most token based platforms regularly destroy their tokens as a way to claiming value by the network. We will not mint new tokens, but only "burn", or destroy tokens. Tokens will be migrated to our Quantum Safe blockchain. Participation in both the ETH and ETC markets can be problematic within the context to exchange participation. We fully expect to offer ETH-tokens and ETC tokens on their respective exchanges. Trading will allow for price parity as the ETH-token will ultimately become phased out as we deploy and implement our Quantum Safe Blockchain. New sales will be exclusive to the ETC-token and repurchases will be available for users holding ETH-token. If regulation is passed that severely impacts cryptocurrency (which is considered highly unlikely as result of current laws and regulations passed within our domicile), we are prepared to offer an "in-house" exchange and separate the value of the token from cryptocurrency.

Network Value

The network and token valuation is based on the principle that a medium of exchange has value between users. As the perverseness of cryptocurrency grows and more goods and services are bought and sold using cryptocurrency as the means of exchange, an increase of liquidity will result. Our strategy will attempt to move (in bulk and new development) the assets of artists into a network available to users of cryptocurrency.

The Network Utility (n*(n-1) users the preceding equation to reflect the overall value of the the network. This concept is widely known but is not clearly understood. The value of the network is that it scaled exponentially based upon the number of participants, known as nodes, in the network. The business and network model that we have implemented recognizes that participants are not a single case node but users participating together. Participants will be rewarded for their common behavior in

the network and as more data becomes available to map behavior, we will implement practices to reward such behavior.

MediaCoin Network Phases

The initial mode of monetization for MediaCoin will be the use and delivery of content. Both Blockchain "Gas", the internal pricing or “execution fee” that senders of transactions need to pay for every operation made on an Ethereum blockchain and data transfer fees will be assessed and included in each total. Monetization will occur as a result of these different Phases.

Phase 1 Network:

Music, Movies, TV, Webcam and Streaming. We are, at the moment, acquiring licenses for music, movie, and TV shows to ensure a full lid of content. Our users will also be able to utilize our secure Webcam services and hence will have access to all streaming media for personal preference and for enhanced business communication (our webcam).

Phase 2 Network:

File transfer network payments and Paywall services. Our secure file transfer of network payments and paywall services allow for efficient and secure resources for users to transfer files. Our paywall services will allow users to preview content but will allow content creators the opportunity to monetize their content as users will have to pay a fee to view the content in full.

Phase 3 Network:

Shareware distribution, payment and licensing, Bandwidth sharing between devices (Share Cellular data for pay over bluetooth, etc), with Tunneling and relays (Tor style, but with 0-4 hops where hops are connections between devices). We will ensure that there is sufficient bandwidth sharing between devices, such as media sharing over cellular networks, to provide an optimal experience using our networks. Using data will also allow users to pay over bluetooth, a significant step in the convenience of payment. Our shareware distribution allows for users to view a trial version of content before purchasing the full version. Content creators will have the opportunity to utilize our Shareware software to both license and accept cryptocurrency payments.

Phase 4 Network:

Bandwidth and relay mapping
Discovery and announce (with gamification examples)
Private transactions between users
Decentralization using blockchain to replace token
Quantum Safe Cryptography

Our Phase 4 network will allow our users the ability to optimize their bandwidth and relay mapping. Artist will be able to announce their additions to the MediaCoin library and because of our search optimization algorithms in place, our content consumers will able to easily locate and purchase content. We have a secured platform for private transaction, primarily focusing on the decentralization of

blockchains to replace tokens and our secure Quantum Safe Cryptography will allow for users to securely purchase streaming media

Market Segments

We have identified a number of market segments:

- Artists who want more control over the sale and use of their content.
- Audio and video consumers who are looking for an easier way to buy media than being locked into an inflated media subscription.
- Media owners who are concerned about content piracy
- Media innovators who are looking for how to meet the demands of their customers.
- Technology, media and telecommunication companies looking to innovate using blockchain and cryptocurrencies.

MediaCoin Tokens

ETH and ETC Network

QMCT is released on the ETC Network, with the ICO address at:

The ETC Frontend address, to perform trades, inspect ownership, check balances, and track in wallet is:

QMCTe is released on the ETH Network, with the ICO address at:

The ETH Frontend address, to perform trades, inspect ownership, check balances, and track in wallet is:

Both the QMCT and QMCTe tokens can used to view the same content. ClassicMask can handle both tokens and both networks simultaneously.

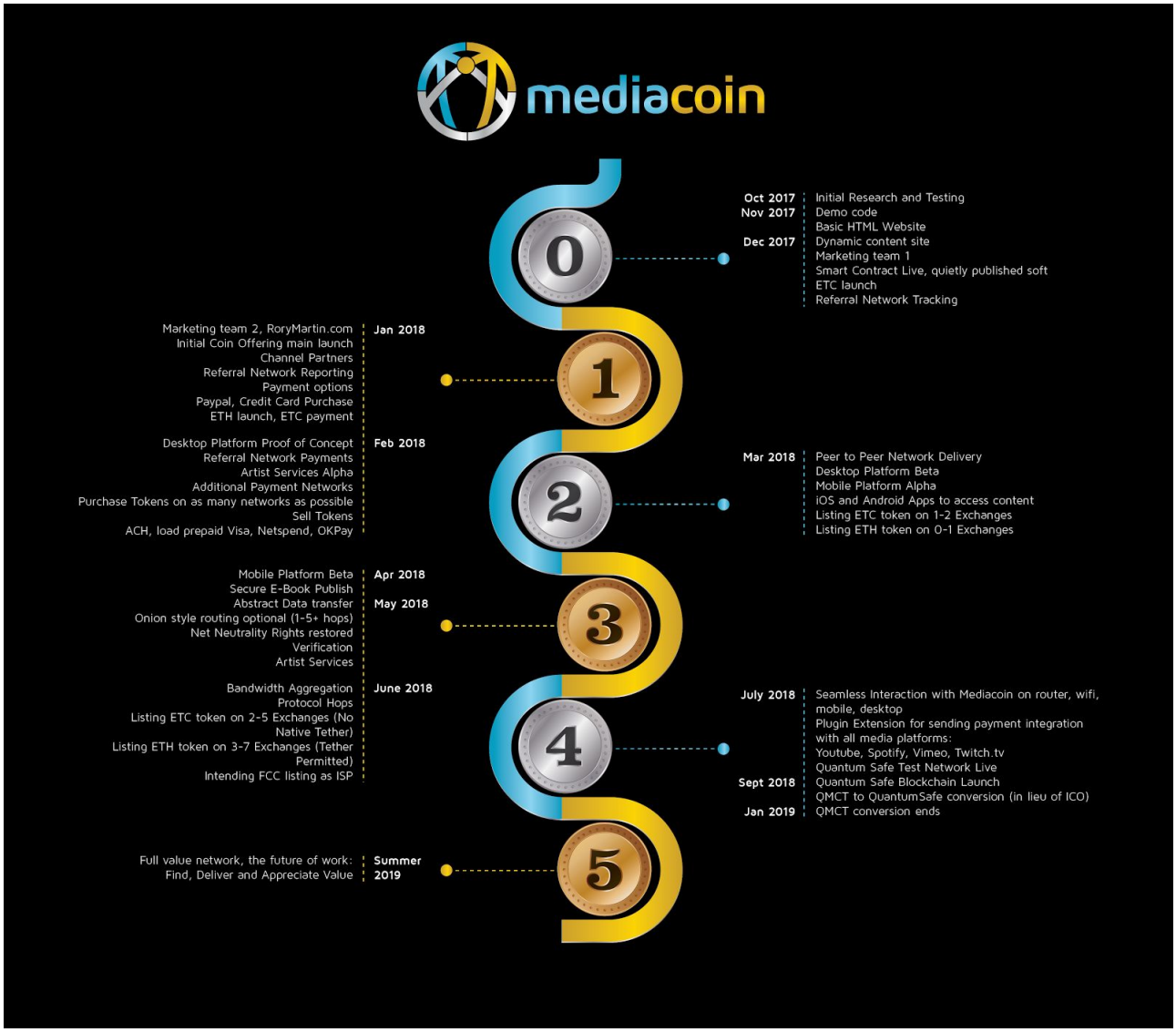
QuantumCoin

When the QuantumCoin blockchain is prereleased, MediaCoin tokens can be used to purchase QuantumCoin before the QuantumCoin launch. MediaCoin tokens will be the main exchange supported transfer of value from Bitcoin and other blockchains to QuantumCoin.

Freemium

Full access to network. Earn tokens by watch ads, installing apps, playing sponsored games, providing personal information that isn't shared, surveys (shared and unshared), participation in promotions.

Roadmap


mediacoin
0
Oct 2017
Nov 2017
Dec 2017
Initial Research and Testing
Demo code
Basic HTML Website
Dynamic content site
Marketing team 1
Smart Contract Live, quietly published soft
ETC launch
Referral Network Tracking
1
Jan 2018
Marketing team 2, RoryMartin.com
Initial Coin Offering main launch
Channel Partners
Referral Network Reporting
Payment options
Paypal, Credit Card Purchase
ETH launch, ETC payment
2
Feb 2018
Desktop Platform Proof of Concept
Referral Network Payments
Artist Services Alpha
Additional Payment Networks
Purchase Tokens on as many networks as possible
Sell Tokens
ACH, load prepaid Visa, Netspend, OKPay
Mar 2018
Peer to Peer Network Delivery
Desktop Platform Beta
Mobile Platform Alpha
iOS and Android Apps to access content
Listing ETC token on 1-2 Exchanges
Listing ETH token on 0-1 Exchanges
3
Apr 2018
May 2018
Mobile Platform Beta
Secure E-Book Publish
Abstract Data transfer
Onion style routing optional (1-5+ hops)
Net Neutrality Rights restored
Verification
Artist Services
4
June 2018
Bandwidth Aggregation
Protocol Hops
Listing ETC token on 2-5 Exchanges (No Native Tether)
Listing ETH token on 3-7 Exchanges (Tether Permitted)
Intending FCC listing as ISP
July 2018
Seamless Interaction with Mediacoin on router, wifi, mobile, desktop
Plugin Extension for sending payment integration with all media platforms:
Youtube, Spotify, Vimeo, Twitch.tv
Sept 2018
Quantum Safe Test Network Live
Quantum Safe Blockchain Launch
QMCT to QuantumSafe conversion (in lieu of ICO)
Jan 2019
QMCT conversion ends
5
Summer 2019
Full value network, the future of work:
Find, Deliver and Appreciate Value

Team

MediaCoin Bios: (full name, title, pic, bio, linkedin)

Don: Chief Executive Officer
Don Morrison began his career in the bank industry with numerous successes in banking leadership, market innovation and operational improvement. In addition to a long career of running financial institutions, he purposely expanded his knowledge into the field of IT. This enabled the capability of development over the last 10+ years, leading solution innovation for countless banking clients. He has helped organizations to refine vertical strategies and re-build global sales and solution to organizations so that they may focus on providing value to existing and prospective clients. Mr. Morrison joined the MediaCoin Team as the Chief Executive Officer in January 2018.

https://www.linkedin.com/in/donmorrison1714/

Ian Smith aka rorschachrev : Chief Technology Officer
Quickly developing projects in the most suitable language under tight budget and program constraints became a specialty. Since 1998 he has written programs in 19 different programming languages for pay, bringing dozens of projects to completion. Ian also worked as a clustering and firewall consultant in Silicon Valley; worked on internet backbone routers at PAIX.net; profitably automated Forex trading for 3 years until 2008; taught Linux at NASA, Visa, Oracle, Boeing and many more.

https://www.linkedin.com/in/ian-smith-20a42876/

Rory Martin: Marketing
Rory has over 17 years of expertise building and running interactive marketing and web design firms. His client list includes small, medium, and Fortune 1000 companies like Target, Redhook, KIRO7, The Seattle

Times, Thompson Reuters, Intel, Microsoft, Classmates.com, HTC, Genentech, Accenture, T-Mobile, and Motorola. His work is focused on creating Social Media Strategies that reflect unique brands and cultures. Online marketing campaigns deliver both measurable revenue as well as ancillary brand building benefits for clients. He helps companies realize the value of social media marketing campaigns and delivers reliable ROI in the process.

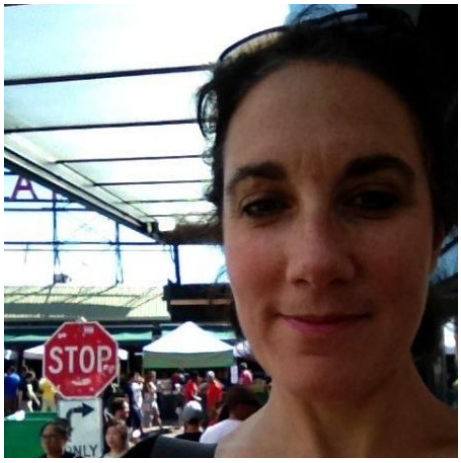
https://www.linkedin.com/in/rorymartin/

Jeff Lam Tian Hung aka jl: Sr UI and Javascript Developer
Founder and Director of Teleo.co, a project management and team collaboration tool for small businesses. Previously Lead Sales Engineer in Asia for Symphony Communication Services, a secure collaboration and workflow technology company that is valued at >USD $1bn in 3 years. As one of the company's first five employees, he has served in a variety of roles including engineering, product design, marketing, and sales.

https://www.linkedin.com/in/jefflamth/

Nadine Krefetz, VP Content
Nadine is focused on designing tomorrow's media experiences. She has been in the digital media space for many years and has worked on over-the-top TV delivery, enterprise content product development and other digital media projects. She has extensive experience managing projects and programs for a number of media companies and technology vendors involved with digital video. She's especially interested in helping media owners transition to using cryptography and blockchain technologies. She is

also a contributing editor at Streaming Media Magazine and writes extensively on technologies that are impacting media today.



https://www.linkedin.com/in/nadinekrefetz/

Broden Staples: Business Development/Blockchain Enthusiast
Broden thrives on understanding client business challenges and mobilizing teams and suggesting options to create valuable solutions that drive business results. Bringing over 15 years of B2B sales management from multiple industry's handling contracts valued in the millions. He has hands on experience with cryptocurrecies, blockchain and trading/programming in Forex markets. Broden currently resides in beautiful Gig harbor, Washington.

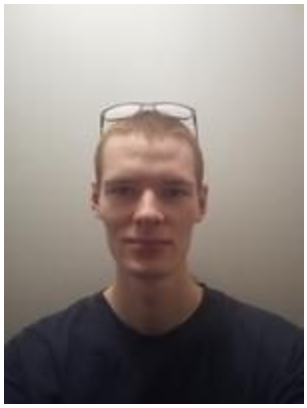
https://www.linkedin.com/in/broden-staples-020b343b/

Garrett Meade aka GP123: Community Director (sent req 1/23)
With almost 20 years of frontline experience working with both end-users and employees, Garrett is ready to ensure a great customer experience. He creates a positive atmosphere and puts people at ease. He holds a BBA in economics from the University of Memphis. Garrett is a champion of and for the people. And he is always at your service!

https://www.linkedin.com/in/garrett-meade-229615152

Envel Lozach David Carliez aka Kireshi: Jr Developer

David, a genuine infosec enthusiast started developing 2016; he is an expect in Junior Javascript/Java and is an accomplished PHP Developer. David received his OSCP license certification the same year he received his Bachelor's degree in Computer Programming. David completed many of his studies in France, and currently resides in Belgium where he is working on projects related to Information Security.



https://www.linkedin.com/in/carliez-david-826599a4/

mstr_choc: Security

MisterCh0c is a security passionate and professional. Previously developer, he's been working as a security consultant for over 2 years doing security assessments in a range of different environments (web, industrial control systems, IoT, mobile). He has contributed to several open source projects over the years and continues to do so.

Appendix A: Phases of Network Payments

Phase 1 Network Payments

The income for our artists will focus upon these factors:
90% to the artist who has created and published the media
3% to the user who has referred the artist
3% to the user referral for the specific referrer
2% to an Artist who provides the referral
2% to the DJ who has placed the artists content on their playlist (or artist if not actual playlist)

If no referral, the unassigned percentage goes to advertising for more recruiting. This advertising becomes the referral partner. Untracked referrals (user deleted the referral code) get smaller sign up bonuses than tracked referrals.

In regards to derivative works, which includes speculative design and copyright varies by media type, we propose the following:

Original content artists will select their fee and any and all derivative works inherit their pricing from the original work. If there is proper attribution and use of 'in network' content, this reduces fees and increases pay. After the licensing costs are determined, the bonus is added to arrive at a total cost. Outside network fees that are not 'normative use' will have overestimated costs at launch, reduced to actual costs and retroactively paid. Regionalization aggregates pre-agreement licensing, cost reduction and fair use will be explored per locality.

5-100% of normal fee, based on 'normative use' interpretation for each media type
10-30% bonus to editor (commentator, remixer, promoter, or other role)
4% bonus of editor Referral for artist
3% bonus of editor Referral for referral
3% bonus of editor playlist or link

Funding Wallets

It is vital for to understand that new users are paid an initial balance for plugin install and account creation.

10-500 Tokens will reflect an initial value of 500 tokens. The incentive by token will decrease as the token value increases relative to US dollars.

There will be a bonus of +5% for any user referral, which requires wallet activation. In addition, the following percentages reflect additional payments:

5% Referral for Earnings (Based on advertising partners, incentives, but not DJ or duplication of other payments)
10% Deposits Referral (Based on our fee, not total)
5% Deposits Referral for Referrer (Matching reward using same calculations as above)

If there is no referral, the initial balance is half the normal rate. Accounts inactive for 6+ months may have their referral payments folded up one layer, as a secondary anti fraud method. It is imperative to note that users who create a new account to only refer themselves. Any policy changes would only be made after simulation and evaluation on the impact to the total network.

Any Television, Anime, Movie show licensed will show the following income:

97% rebate for prepayment
1.5% Referral for content
1.5% Referral for referrer

Any Television, Anime, Movie show income published will reflect the following income:
90% to the artist that published the media.
4% Referral for artist (Introduction of artist)
3% Referral for content (Link to content)
3% Referral for referral (Introduction of content referrer)

Every data transfer will have a delivery fee, based on storage, requests and bandwidth. The license key will be delivered after the data transfer fee is paid. Since all content is encrypted and licensed, sharing files for upload will be directly paid starting in Phase 2. A healthy network in Phase 1 will use prepayment for file storage and sharing.

Data transfer (phase 1):
90% rebate for prepayment
5% Referral for content (DJ, outside link, reviews)
5% Transport Protocol Handler (supernode, DHT node, IPFS DHT, etc that supports mapping from request to delivery. Responsible for key delivery upon completion)

Phase 2 Network Payments

90% for file delivery, split per chunk of data.
5% Referral for content (DJ, outside link, reviews)

5% Transport Protocol Handler (supernode, DHT node, IPFS DHT, etc that supports mapping from request to delivery. Responsible for key delivery upon completion)

Gas Estimates

Initial Transaction costs ("Gas") are calculated by processor time, storage, and various factors using a specific quantitative metric. Phase 1 will, at minimum, rely upon direct costs for Gas payments. Aggregating transactions will lower costs, and urgent transactions will increase costs. Multiple techniques will be employed in Phase 2 to lower Gas costs for users and the network as a whole.

Pay Wall services

Many news and article sites require direct payment or an adblocker to access their content. Since our user base already has a browser plugin, very low costs, opt-in behaviors, and easy payment options, MediaCoin is positioned to act as a payment gateway for "pay per view" or "pay for access" services. While many of these services require a subscription, we can seamlessly function as an opt-in behavior system or token based payment method.

Phase 3 Network Payments

5% Referral for access (no pay for local discovery, pay for DApp mapping of access, etc.)
5% Transport Protocol Handler (exit Gateway Handler for request, may include DNS, bundling UDP in TCP, packing files, etc)
5% Traffic Tunneling per hop, by client request (0-3 hops)
75-95% for network access, pay per MB transferred

Software Licensing

In general, software licensing is a more complex topic because of the multiple type of licenses that must be supported. The development of a secure software delivery platform is complicated since there must be deep integration within the software product. A purely superficial license key solution is easily bypassed through software disassembly. Office software, iPhone and Android apps, Shareware, MMORPG game titles, online console games and more will be supported. However, licensing agreements will often need to be established first. Subject to the terms of the content creator, we will share what is fiscally viable for download and promotion.

Phase 4 Network

Private transactions on Quantum Safe Blockchain

The creation of blockchain is dedicated to a network is a significant step forward in the long term advancement of the network. Tokens will be initially redeemed for transfer at ICO rates, and later at market rates. This conversion is the only case that any tokens will be destroyed by the network.

Decentralization using blockchain to replace token transactions

MediaCoin Tokens will be maintained and traded indefinitely. Moving operations into Blockchain ensures continuity of the network and immutable resistant to outside interference. Guidelines protecting users and artists should be well established, with multiple access points. Blockchain based publication creates further opportunities and more freedom in implementation.

Proof of Work for network shares in GPU will be the bulk of the initial miner reward. The goal is to transition the entire network to collection and distribution of transaction fees without mining. Mining routines in GPU will mimic transactions with optimizations in mining software lowering transaction costs.

Appendix B: Quantum Safe Blockchain

Quantum Risk

Nov 10, 2017 IBM Announced their 50 qubit quantum computer (https://www.technologyreview.com/s/609451/ibmraises-the-bar-with-a-50-qubit-quantum-computer/ quantum computer.) Sweden contributed $1 billion in funding towards their development of a 100 qubit system. Unlike D-Wave's 2000 qubit system (https://www.dwavesys.com/press-releases/d-wave announces d-wave-2000q-quantum-computer-andfirst-system-order) the IBM quantum computer is capable of performing Shor's algorithm, which is capable of solving Discrete Logarithms. This is a NP-complete problem, solved in polynomial (P) time using Quantum Fourier Transforms (QFT).

The main limitation of quantum computing is that problems must be solved "all at once" and can't be solved in pieces the way silicon transistors currently do large number math. The second limitation is decoherence, where the system falls apart before an answer has appeared. Thirdly, answers are probabilistic, with some noise and chance that a wrong or "no answer" will appear.

The current simulator and cloud computing offered by IBM uses a mixture of Python and their Qasm (Quantum assembler) language. (https://quantumexperience.ng.bluemix.net/qx/experience) The fundamental question on a system capable of solving Discrete logs and breaking All Modern Cryptography is mostly a question of "when" and not "if" it can happen. The underlying hardware used by IBM is nuclear magnetic resonance (NMR) machines, which are present in medical labs and university systems. Once the methods are figured, it is likely that many independent labs will be able to perform quantum calculations.

If some of this research is able to leap forward based on the D-Wave designs (even though Niobium magnetic method and the NMR method are much different) then a quantum computer to break most cryptography is likely within 1 to 3 years. As larger and larger qubit arrangements become common, more and more cryptography will be solvable by such a system. If the techniques pioneered by DWave are not applicable, then a 3-6 year time frame is more realistic.

Quantum Migration

After quantum computing, the "best solution" offered among the Bitcoin community so far is creating all transactions in pairs. The first transaction is a spend of bitcoin, and the second transaction moves to a new address to prevent a quantum computing attack against the public keys that were exposed. The "second best solution" is moving all bitcoin to a series of Central Authority Silos, which would store the balances in databases and have some sort of 2 or 3 factor authentication requirements, allowing registered users to safely store and spend their bitcoin. Neither practice would work with Ethereum,

unless Smart Contracts were created without "owner" permissions and the authentication to the Smart Contracts do not involve modern public-private cryptography.

The most effective solution overall is an early migration. Quantum Safe Cryptography can be implemented now, and quantum safe blockchain can be developed within the next three to six months The author has spent some time on this, attempting to create a smart contract system with privacy and quantum safe libraries. In the budget projections, money is allocated to mathematicians and researchers in order to ensure accuracy, design attacks, and countermeasures. It is presumed since blockchain can be upgraded, new algorithms will fix any inadequacy revealed in the future. However, this proposition is not entirely valid unless the address and balance calculations are backward and forwards compatible.

In Bitcoin:
• sec256k1 "private key" which is a point on an elliptical curve https://en.bitcoin.it/wiki/Secp256k1
• sec256k1 "public key" which are 2 numbers, related to the elliptical curve
• a SHA256 hash of the public key
• a RIPEMD160 hash of the SHA256 hash

In Ethereum:
• sec256k1 "private key" which is a point on an elliptical curve
• sec256k1 "public key" which are 2 numbers, related to the elliptical curve
• a SHA3.keccak256 hash of the public key, truncated to 160 bits (non-reversible, even if the tech existed)
• Contract addresses are SHA3.keccak256 of RLP(nonce+sender_address), truncated to 160 bits. There is no public or private key for contracts

This data cannot be altered and still maintain the private key access to funds, which essentially locks the address scheme in place since the address is based on the public key, and the public key is revealed in transactions. In other words, after exposure the funds are accessible to anyone or to no one. Bitcoin could continue after upgrading to prevent quantum attack, but upgrades to the protocol will leave old accounts vulnerable until they perform transactions under the new architecture.

If we use a token instead of a central authority, we have access to cross chain transfers on exchanges as well as blockchain to blockchain. To facilitate a transition to a quantum safe blockchain, we are creating a custom code to be used where users can "burn" tokens and receive quantum safe coins on the new chain. The "burn" to transfer mechanism will be left unimplemented until the quantum safe mechanism is in place, tested and then the contract "library" will be upgraded with the function. In the meantime, contract to contract transfers are blocked by an implementation of Dexaran's ERC223 proposal (designed to prevent Ethereum loss). After migration upgrade, contract to contract will be permitted and tools will be made available making the process user friendly and will increase monetization.

Appendix C: Zero Sum Game

Cryptocurrency markets are a "Zero Sum Game" similar to stock equity markets. Every dollar 'earned' in cryptocurrency and equities trading comes from another trader's 'loss.' A healthy ecological system and a healthy market bear similarities as "Living Systems," as detailed by James G Miller in 1972. Cryptocurrency, especially as a fledgling market, must be intentional, cognizant and careful to obey the Natural Limits (Natural Capitalism) as the system grows. MediaCoin is focused on detailing the financial systems required to make cryptocurrency a sustainable system with lasting growth.

The main difference between the markets is the input and output to the whole system. Equities receive system input as funds from IRA, mutual funds (especially tax free profits as "passive foreign investment instruments") and indirectly through some option vestment plans and dividend payments to shareholders. Cryptocurrency has direct goods and infrastructure building but both systems generally remove more value through fees than the direct investment in liquidity needs.

With Cryptocurrency as a Zero Sum Game, it is important that the output costs are minimized and the input income is greater than the output costs. Without a careful consideration of income > cost, then the resulting market is often referred to as a speculative bubble because it relies entirely on new investment to fuel the ongoing costs. When the investment input slows, returns diminish and large withdrawals at that stage will cause a speculative collapse. When income is greater than cost, the investment input is attempting to capture long term income with equity investment. For the health of the overall system, it is important that projects with costs vastly exceeding income collapse quickly to avoid risk and weakness in the larger system. Equity investment in infrastructure is a necessary step to capture long term value, but it can not fix situations where cost exceeds income. If a large investment is able to capture a lead in a marketplace, the project must gather value and convert it to income, or sell their network to a system that can gather value.

Appendix D: Aggregate Cost Averaging and Behavior Valuation

The micromanagement approach to costs and income is very significant, because it is impossible to lose money on every transaction and yield an overall profit. The converse statement is true, it is possible to accrue revenue on every transaction and not yield gross profit due to infrastructure, licensing and total system costs.

MediaCoin takes the approach that earning income on every transaction while minimizing infrastructure costs will yield total system profit. Unlike most projects, MediaCoin will avoid aggregates of cost, profit and transaction volume for a total system gross profit. Many projects take the approach of advertising "screen real estate" to gather income. The expected income is based on the total screen real estate of all combined users viewing advertisements. If the advertising income is higher than the total system costs, the project yields gross profit. As the cost of providing services to each individual user is minimized, the system costs go down. If the advertising yields a profit to the advertiser, the advertising becomes sustainable and so does the projects that rely upon advertising for income. It is not possible to overstate the profit significance of only providing services to each user based on the actual gains to the entire system. Each transaction and each user will be profitable, with the exception of initial cost of user

acquisition. Infrastructure and some licensing will primarily be paid for with the Initial Coin Offering and ongoing sales of Tokens.

Subscription models for content have disproportionate usage. 52% of all adults who read the news never subscribe to a particular newspaper. The delivered value to users who pay for monthly subscriptions but infrequently use them will lead to user dissatisfaction regardless of quality of service. Creating artificial barriers to cancellation creates a secondary consequence of alternative markets. As the trend of cellular service requiring a 1 year minimum contract progressing to a 3 year minimum contract, the market for pay-as-you-go service without cancellation barriers grew in correlation.

MediaCoin's use of Tokens to accurately represent value allow us to map costs and offer peers payment for lowering costs. The main cost for streaming sites is clearly bandwidth, and members who offer their bandwidth to peers can be paid accurately per megabyte delivered for data transfer. Use of bounties and tokens for services will allow us to spend tokens instead of venture capital for behaviors that increase the value of the network. We intend to reward our community for contributing to our success, rather than exploit it as a no cost means of providing support without reward.

Accurate Cost Measurement and Behavior Valuation will allow our company to recognize inefficiency and reward efficiency while increasing the total value to all network participants.

Robust decentralized verified network of master session handlers to convert, encrypt and deliver data.

In order to comply with laws world wide content will be tagged and accepted or rejected by masternodes and each other connecting node. This allows compliance with local law to prevent illegal content