IRIDIUM

Whitepaper
V3

Contents

Abstract

Hey, sometimes you need a stable, secure, anonymous coin to handle transactions. There's a lot out there to choose from and we think Iridium is a great choice! Iridium assures your coins stay valuable from now and into the future. From our strong stable network of 12+ global nodes to our diverse eCommerce focused application set, we have all your use cases covered.

Like Iridium the element[1], this coin is rare; only 25 million will ever be made. Early miners reap the most benefits, with 12.5 million IRD being awarded the first year (September 2017-September 2018). Miners are protected from unfair difficulty increases by a unique block-focused difficulty retargeting algorithm. This means you're ensured a stable mining reward.. yes, even you 2-GPU miner person!

We think our strength lies in our community. From our integration-oriented development team to our enthusiastic user base; the Iridium community has come together to form some amazing products in the past 9 months. Our integration with Wordpress and Woocommerce brings our coins capability to over 50 million sites! Our brightest and best work is yet to come.

You won't see our community leaders mindlessly tweeting about vapor-partnerships that never result in anything. They're focused, heads-down, working hard to bring the community the best product for transactions the crypto world has to offer.

Finally, we are putting up the "Investors Welcome" sign! This is a no-ICO coin; we don't have a shady starting point like many ICO coins out there. Our coin also had no-Premine; you won't have a large group of insiders looking to whale splash this coin into oblivion. You're looking for a healthy, small supply, low-market-cap coin that can be used for anonymous transactions, so hop onto our several exchanges (TradeOgre, MapleChange, Altex and Crex24) and trade into IRD.

We aren't here to change the world with crypto, we're here to change your mind about crypto. (too strong? yeah..)

[1] http://www.rsc.org/periodic-table/element/77/iridium

TLDR

Let's be honest, we think reading a whitepaper of an crypto-currency in 2018 can be a rather joyless task. So, dear crypto-currency whitepaper reader with your super valuable time, here's a TLDR for you! Give the the Abstract and TLDR a read through and you'll get a pretty good idea of what Iridium offers. If you need more details though, go ahead and read the rest of the Whitepaper!

Also a note about this whitepaper: We tried to make it easy to read. Please do not mistake a friendly tone for a lack of seriousness. Many whitepapers sound so dry and boring, and for what! Let's make these things interesting again.

Iridium Summary

An anonymous, privacy-friendly, fairly-mined crypto coin with low-supply, high-availability, best-in-class security and an enthusiastic community.

 Fully Anonymous - Based on the venerable Cryptonote protocol, users of the coin have full protection against transaction visibility.

 Privacy Friendly - TOR based nodes in the roadmap, we've already vetted this out and are looking for a Q3 2018 launch of some privacy friendly nodes for TOR users.

 Pure POW - All users are equal, no master nodes that make small holders feel insignificant. If you own Iridium, you are equal to the largest whales.

 Fair-Mined - ASIC-resistant mining algorithm that lets CPU/GPU miners keep the network going. Development team commitment to following the latest mining trends.

 High-Availability - 12 nodes globally distributed with anycast DNS ensure that you're going to be able to send your coins without delay. A true rarity amongst community coins, Iridium has strong network architecture beyond what other community coins can claim.

 Security - Mining attacks are a thing of the past with Iridium. Our strong security model, vetted by the top consensus algorithm experts in the field, ensures protection against difficulty spikes.

Developers, Developers, Developers - Developers based in the EU and U.S.A with deep creative experience; our team has shown resilience and fortitude in the face of challenges. We prize our can-do spirit and our product has a lot to show for it!

Community Enthusiasm - A global community with fantastic enthusiasm, Iridium is a chill environment that prizes honesty, hard work and a collaborative attitude above all else. There are no heroes here.. just people who value teamwork.

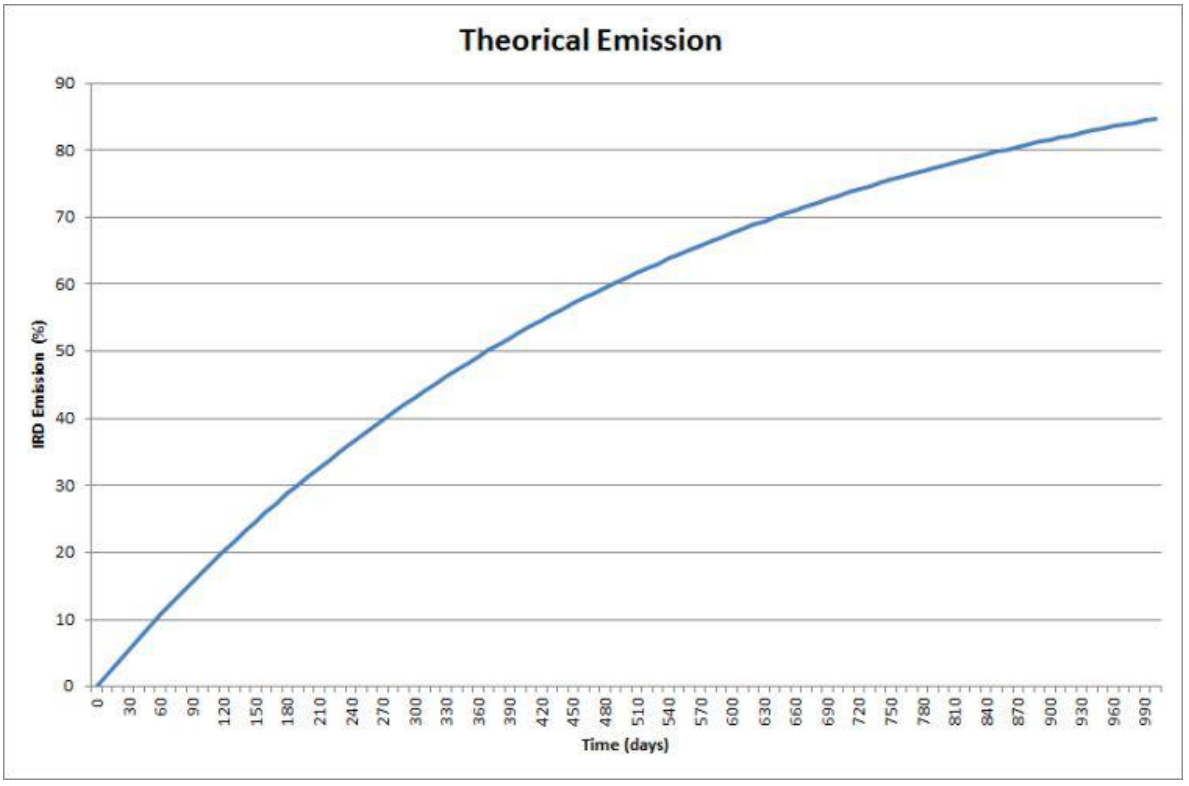
Iridium Specifications

Let's see those sweet sweet deets!

- Name: Iridium (IRD)
- Launch Date: September 04 2017
- Mining Algorithm: CryptoNight Lite Variant 1 (As of May 1 2018)
- ASIC-Resistant
- Protocol: CryptoNote
- Proof Of Work (POW)
- No Pre-mine
- No ICO
- Total Coin Supply: 25,000,000
- Confirmation Time: average of 3 minutes every 60 blocks
- Difficulty Retargeting: 175 seconds
- Emission rate: 12,5 million coins being distributed in the first year
- Block-by-block difficulty adjustments: Zawy's LWMA[7] difficulty adjustment algorithm
- Blocksize: Variable (Recalculated on Previous State)
- Max Block Size: Bound by size of previous two blocks, allows growth without bloat.

Iridium Features

- Fully Anonymous Cryptocurrency
- Stable, Global Distribution network backed by one of the largest ISPs in the game
- Fully eCommerce Enabled
- Capable of being used on over 50 million websites via WooCommerce
- Dedicated Development team, fully versed in crypto, eCommerce and big-data.
- Enthusiastic Community - Well maintained Discord and Telegram groups



Emission in days

Roadmap

If you're here for that sweet sweet Iridium ROADMAP; you're in luck. Here you go.

Development Roadmap

May 2018 - White Paper, Website launch
June 2018 - WooCommerce PHP Plugin Beta (Local Node)
June 2018 - Java API Complete
June 2018 - Remote Nodes available for public use (Setup for Woo, Mobile, Web wallets)
July 2018 - Python, PHP and NodeJS Wallet API
Q3 2018 - Commerce Enhancements
Aug 2018 - Wallet and Daemon Speed Improvements
Aug 2018 - WooCommerce PHP Plugin Remote Node
Sep 2018 - Web Wallet Beta
Sep 2018 - Coingate Beta
Oct 2018 - Web Wallet Production
Oct 2018 - New Mining Algorithm
Nov 2018 - Coingate Production
Dec 2018 - Mobile Wallet
Dec 2018 - Bisqord.network Integration

Long Term Crypto Roadmap

Q1 2019 - Tor Nodes
Q2 2019 - Scale Model Implementation
Q2 2019 - Aim to become supporting baseline for all Cryptonight/note coins
Q3 2019 - Consumer Grade Features such as Cancel, Refund

Introduction

Today Bitcoin is synonymous with cryptocurrency. Bitcoin was the first implementation of blockchain technology that allowed cryptocurrency to be traded and trusted as freely as fiat currency.

The decentralized nature of Bitcoin development is one of the major features of Bitcoin. Academics, economists and computer scientists were inspired to contribute their own improvements to Bitcoin and the cryptocurrency world in general.

One of these improvements is the Cryptonote protocol. A group of cypherpunks got together with the goal of creating a truly anonymous currency that was open to improvement.

And that's where the story of Iridium begins! Iridium takes the next step in the development of a decentralized cryptocurrency. We aim to be more than just another cryptocurrency. We see Iridum as a powerful global platform for commerce transactions; as a way for normal people to use an anonymous cryptocurrency.

In the original spirit of Bitcoin, we're also interested to see how the community can come together to solve problems, make improvements and reach our goals. We aim to be different than other coins out there; we want to push the boundaries of what Crypto could be in an entirely organic way. Iridium will do this by pulling together the best qualities cryptocurrency offers today. We'll also organize the community and development to incorporate all future improvements to the crypto world.

People are power; and we can only do this by cultivating the community! A community is nothing without people. Extra effort is put into the curation and development of community members and to allow the best ideas and efforts to float to the top.

Core Principles

There are a handful of core principles that Iridium seeks to support. “People are Power” was our first slogan and it means more than just some cool sounding phrase. Iridium chooses to embrace and enshrine the following principles in our approach to technology.

A Commitment to an Open Community

An open community means that people can get together to further the development and reach of Iridium without relying on dictates from one central authority. There are some core development team members that serve to provide a “trusted” face to Iridium, but by and large we rely on the contributions of dozens of individuals for our existence.

Iridium focuses on contributions and effort from individuals and teams. Individual contribution is critical to decentralized projects. Iridium wants to welcome new people, and build a community that encourages contribution from anyone that wants to be a part of the project. A contribution is more than just someone saying an idea in a discord room; a contribution is a tangible unit of effort that moves Iridium forward. The community team will do our best to elevate those individuals who have provided tangible effort.

Good examples individual contributions to the Iridium space are

- creation of this Whitepaper
- the Ird.Cash website
- Java Integration API

Bounty System

A bounty system is a great way for us to encourage the open community and efforts from individuals! Creation of bounties can be done by anyone in the community provided they follow through on a few rules. Bounties can help individuals “know” how to contribute to Iridium by detailing what needs to be done and also by providing for a small acknowledgement for their contributions.

We understand that not everyone is motivated by “getting something”, for those individuals we allow them to “donate” their bounty in any way they choose.

Flexible Protocol Updates

Iridium will stay current with updates to all the various protocols that we use. Improvements in technology excite all of the core team members and we want that commitment to show! We've incorporated new technologies like the Linearly Weighted Moving Average (LWMA) algorithm[7] and other security improvements that allow for difficulty retargeting.

We aren't afraid to hard-fork when necessary; our community team puts extra effort into ensuring that all pools, exchanges, and miners get notified and supported when a hard fork takes place.

Ecommerce Oriented

In the few short months that Iridium has been around, a huge success story has been how the community got together to define ecommerce as a goal for Iridium. We are dedicated to growing use of the coin via electronic commerce.

Now it may be difficult to consider an anonymous token as a good candidate for electronic commerce; after all, how else will you help someone create a chargeback or refund. And is it really safe to receive money from an unknown source?

We're going to help solve some of those issues. Iridium is targeting quarterly Commerce Enhancements to our protocol.. We aim to be one of the few anonymous tokens that can also be safely used for Commerce transaction.

And lastly, how about something tangible. As of May 2017, Iridium has the potential to be used on over 50 million (yes 50 million) websites with the WooCommerce/Wordpress integration capability! Not many coins can claim that kind of upward momentum!

Iridium aims to connect

Connectivity is another key principle for Iridium. What does that mean? It means that Iridium aims to connect. Coins that have the best integrations, do the best in the market. A good integration story means that your coin can be adopted in marketplaces and other use cases. Without integration, you have no users!

Iridium is dedicated to creating a healthy ecosystem of integration API's, plugins, and applications to keep the coin growing. It's part of our long term vision for this coins success.

Iridium - A Modest Giant

A coin with this kind of low supply gets people very excited. There are some other qualities that we think you should keep in mind about the coin. Modesty is attractive.

Fairness means No-ICO, No Premine

With Iridium there was no ICO, no pre-mine and no token distribution.

Say what?

“Why wouldn’t you take advantage of the ICO craze? You wouldn’t be faulted for that!”

Starting on a level playing field is crucial to being “fair”. We’re a decentralized cryptocurrency with a low supply. Having a pre-mine would give a first mover advantage to someone! We saw that there was room in the market for a coin that didn’t try to moon on day 1. We also saw there was room for a coin that actively tried to ensure a fair playing field on day 1. Iridium was designed without these Day 1 advantages so that everyone had a shot.

Having an ICO or Pre-mine is fine... for other coins. If you’re looking for the hottest ICO, look elsewhere. We both know you can get plenty of that sweet ICO profit on the market. Iridium is a community coin and we want to maintain that community spirit. So you have everyone starting from a fair playing field. People are Power!

Iridium - A rare metal and a rare coin

So, 25 Million Coins? What’s the big deal?

On the surface you might think that a low supply coin is going to yield a high price per coin. While that might be true, we think there are some deeper reasons that a low supply coin can benefit users.

A low supply coin can keep the community of users smaller and close knit. There are a lot of use cases for a coin where you want to have the trust of knowing who is involved while staying anonymous. It could be easy to get lost in the shuffle for a larger coin, but we think that Iridium stikes a nice balance between size of market and size of community.

There is a simple supply and demand law in play as well. Low supply can be upwards pressure on price. It can also make it harder to come by. We’re tweaking the formula to make sure we can keep the coin as liquid as possible by providing airdrops and giveaways where necessary.

There are industries out there that could benefit from a price representation that skews larger. Larger supply coins could attempt a 1/1 USD price ratio. A smaller supply coin such as Iridium would look to be adopted by a market that loves to be priced using low magnitude numbers. It's strictly practical; big-ticket items such as cars or hourly services, to be transacted with more accuracy (less numbers to enter) and less fuss (less decimals for use).

Finally, we know that the price will be a little lower for the first 18 months while the mining returns are high. 12.5 million coins will be delivered to miners during the first year of this coin, and that's a ton of supply heading out early. This should keep the price range relatively stable as new markets look to adopt Iridium. A stable, well mediated price can ensure happy users and smooth commerce transactions.

Use Cases

Iridium has a fairly simple set of use cases compared to many crypto currencies out on the market. There are 4 problems that we look to solve with Iridium.

Fair-Mining Investment

You're looking for a high-risk and high-reward opportunity with a small market cap coin. You want to use some of your spare GPU/CPU mining power on a coin that still has good returns. You want to mine for a coin that provides a fair-mining opportunity and doesn't let giant miners push out the small ones.

Commerce

You need a way to accept crypto as a payment method on your Wordpress or eCommerce store. You need to use a coin with committed and focused development towards an eCommerce solution. You're not into the idea of centralized payment networks and want to keep support for a coin that is truly anonymous. You're looking for a coin that has a stable global set of nodes.

Anonymous Transactions

You're looking for a safe and easy way to transfer value from one person to another. You want to make sure that you have the right support if something goes wrong. You're probably also looking for a coin that has a web wallet and mobile wallet so that you don't have to download the blockchain every time.

Extensibility and Involvement

You have skills and talents in development, documentation, writing or design and you'd like to contribute to a community that needs them. You want to support a distributed development concept. Iridium provides a lot of mechanisms for integration with outside technologies. We have a dedicated integration team creating API's for public consumption and integration into third-party products. And our dev team brings over 50 years of experience in B2C and B2B technologies. This blockchain is in the real world.

Let's talk tech!

Finally let's take a walk through some of the technical features of the Iridium platform. Iridium is based on the venerable Cryptonote algorithm, a top shelf protocol in use by many super-stars of the cryptoworld! Using this algorithm gives Iridium a ton of super features. Our developers are building new features into Iridium that aren't found in Cryptonote, but much of the foundation of Iridium is based in Cryptonote. If you want to learn more about that, be sure to read those protocol papers.

How is it Anonymous?

Iridium uses ring signatures to achieve untraceable payments[14]. Ring signatures allow untraceable payments by combining multiple individual keys for verification of a transaction. This is an improvement on Bitcoin, as Bitcoin only uses one key. Iridium has multiple users sign the transaction; now the outside world can't tell who it came from! You can see who "may" have participated but you'll never know the true sender.

This does mean that an Iridium users public key might appear in many other transactions; transactions that weren't their own! It's a feature :)

Iridium also uses Cryptonote technology to produce single-use one time keys when sending transactions. These single-use one time keys are derived from the sender's original public key along with some random data pulled from the ether. The keys in the transaction will be different every time someone sends funds. Nice!

Iridium's global network of nodes also allows for some integration with privacy focused networks. TOR nodes are currently in testing. This gives users the optional ability to protect their IP addresses to be hidden.

Reward System

Iridium uses a Proof-of-Work (POW) reward system based off the CryptoNote protocol. ASICs capable of mining on Cryptonight algorithm came into play in April 2018, so Iridium chose to use and replace the Cryptonight algorithm with the Cryptonight Lite Variant 1 algorithm. Cryptonight Lite Variant 1 is ASIC-resistant and in use on many other coins. Users with moderate hardware can mine the currency. Cryptonight Lite Variant 1 allows Iridium to be mined on both CPU hardware and (more efficiently) on GPU hardware.

POW is still considered to be the "gold standard" of rewards mechanisms. With a POW coin, the network is secured by the mining hardware. Thus we are able to stay platform

agnostic. We choose to avoid proof of stake (POS) mechanisms in comparison as this requires one to "buy into" the network.

As of 2018, ASICs have started to move into some more alt-coin focused algorithm. This could potentially have a downward effect on adoption of a coin since mining rewards would go into less users hands. It could also have an upward effect on the price since those ASIC miners would need to move their coins on the market to sell in order to recoup the price.

The plan for Iridium is to stay ASIC-resistant as long as ASICs are seen as high-end hardware. For 2018, Iridium will change algorithms in order to stay ahead of ASICs.

To be clear, we take a neutral stance on ASICs in this whitepaper, but the community does have it's own opinions on the matter. If the community and main devs coordinate a change in policy, a hardfork adapting the new ASIC-policy will follow.

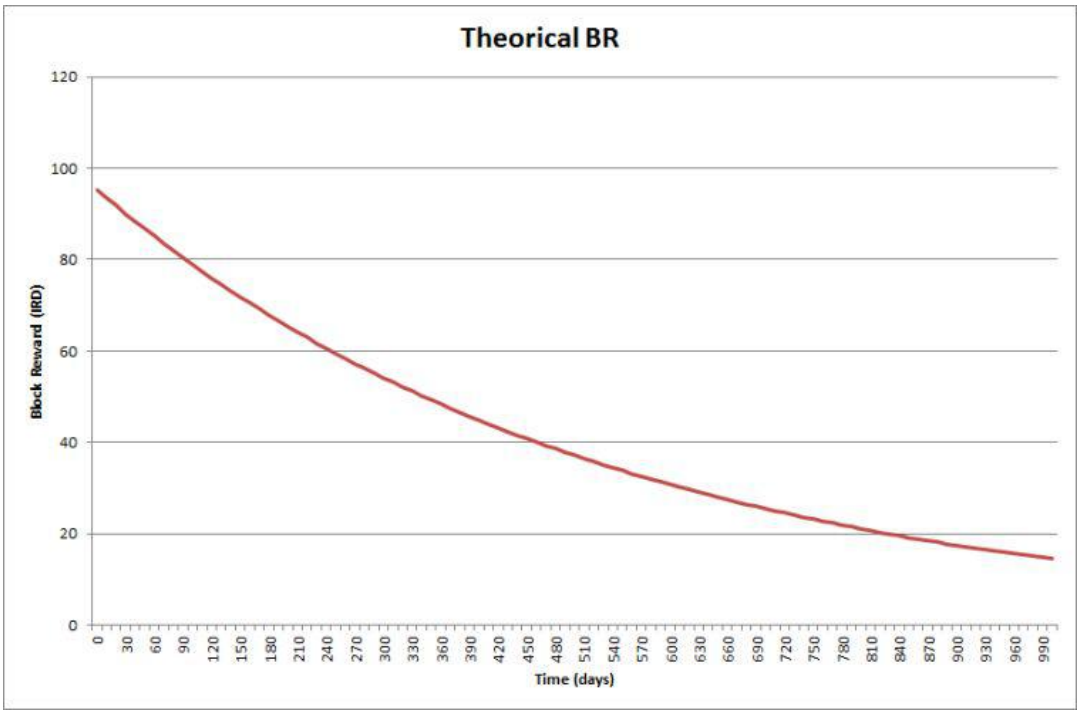
We hope to show that our decision to use POW, in a general way, was motivated by the desire to allow many to participate. You need only bring your GPU to participate with Iridium.

Emission

What is the ideal rate of emission? It's unclear at this point. Iridium decided to play with the existing formula and went with a high emission for the first two years. Year 1 would release 12.5 million coins, while an additional 5.5 million would be released in Year 2. Several benefits may follow from this approach.

Early adopters could be rewarded with large amounts of coins. Those individuals would have a vested interest to make sure Iridium succeeds. We are hoping early adopters of the coin can step up and put effort towards that success.

Since high supply might mean an early lower price in the first two years, we anticipate a more stable rise in value over the life of the currency. We are hoping for a low-volatility store of value that allows users to transact without fear of a fluctuating price.



Blocks reward in days

Adaptive Difficulty (LWMA)

What is Linearly Weighted Moving Average (LWMA)? LWMA allows for the protection against sudden hashrate variations including "hash attacks". The Algorithm ensures that a block is mined every 175 seconds on a window size of 60 blocks. Big miners can no longer come in, mine and leave the network with a high difficulty to resolve. LWMA allows the entire network to react very fast in case of miner attack (2 or 3 blocks). What does this mean? Small miners and big miners have equal weight in this game.

Encryption System

Public, and private keys in Iridium are generated with elliptic-curve cryptography. You can learn more about elliptic-curve cryptography at the Standards for Efficient Cryptography Group (SECG) [http://www.secg.org/].

The Diffie-Hellman exchange protocol variant is also used to generate the one-time keys used when sending transactions. This enables the sender to appear to be unique each time a transaction is conducted.

When generating a transaction, Iridium uses random data in conjunction with public keys. This ensures an additional level of security over traditional public/private key security.

How An Iridium Transaction Works

So you want to send some IRD.. Cool - here is how it works!

The sender of the transaction combines multiple items to get the transaction "ready to be sent". These are just the items that are needed to show the sender is who the sender is. We use the private key, the transaction public key, a random generated number, and the amount of IRD in the transaction.

But now we need to see that the receiver is actually the receiver. It's only fair right? So we create a randomly generated number with the transaction public key, the amount, and the receiver's public key.

After we have all the stuff needed to "address" the transaction, The sender can finally sign the transaction, and append all this stuff gathered to the ring signature at the end of the transaction.

Time to send it! Let's broadcast! Who's listening?

The Iridium network of nodes is out there listening for transactions on open upnp ports listening on default port 12007. If a node receives your transactions, it starts to run validation checks on it! If the transaction passes it's mined accordingly.

Once a transaction has been mined it's added to the blockchain. After the transaction has been on the blockchain for 20 blocks it's considered to be confirmed at that point.

Oh yeah - Your wallet also receives a copy of this transaction. Your desktop wallet is also one of those notes on the network! Keeping all these open nodes out there contributes to the decentralization of the currency. Your wallet then uses a private key or a view key to check all the blocks, and to determine if you received any funds. All received funds are then stored on a local ledger in the wallet. If the local ledger isn't present in your wallet, then the wallet will then start the work of rebuilding the ledger based off of the users private key.

Acknowledgements

We acknowledge all members of the Iridium Community for their continued involvement and focus in this successful endeavour.

Special thanks to the following for providing imagery.

- Idea by Stephen Plaster from the Noun Project

Appendix

Original Iridium Whitepaper

For historical purposes:
https://docs.google.com/document/d/1Xb9u4_k_QzolUh9DTQSLxSATYdHxGdFB7cr7bRzYwhw/edit

Who's Involved?

Core Members

The core members help do things like the paperwork, pay bills, keep people happy and all the "business things". Noone owns Iridium. The community at large contributes. If you need to check in with someone though who's "official" at Iridium, reach out to Shaun or Steve.

They both prefer to stay quiet and heads down. Steve knows a lot of C++ and Shaun knows a lot about software development management, marketing. Both are enthusiasts of Blockchain and software in general and both of them are learning a ton as they go along.

Technical - Lead Developer (Steve) - steve@ird.cash
Global Development Coordinator (Shaun) - shaun@ird.cash

No fancy pictures. No Marketing Buzzwords. 100% Organic Technology.

Community Contributors and Leaders

Iridium wouldn't be where it is today without the help of the standouts and leaders. We've listed a few here! Thanks a ton for all your contributions!

Cryptoguy - Helping us keep the thing running
Datapotomus - Got the website and whitepaper going
Daclasen - Java and Integration genius and knower of all things Docker, Beer Drinker
Seymoura and Comfuzio - Enthusiast and Energy guy in the Discord
All Early Miners - You kept it going
Original Dev - lol

References

[1] https://cryptonote.org/
[2] https://cryptonote.org/inside
[3] https://cryptonote.org/whitepaper.pdf
[4] https://bitcointalk.org/index.php?topic=2150442.0
[5] http://cryptonote-coin.org/
[6] http://ird.cash
[7] https://github.com/zawy12/difficulty-algorithms/issues/3
[8] https://www.chainalysis.com/
[9] http://www.secg.org/sec1-v2.pdf
[10]http://www.secg.org/
[11]https://iota.org/IOTA_Whitepaper.pdf
[12] https://cardanodocs.com/cardano/proof-of-stake/
[13]https://nuls.io/pdf/NulsYellowpaper1.2.pdf
[14]https://cryptonote.org/inside#untraceable-payments
[15]https://www.torproject.org/index.html.en
[16]https://dotnetrussell.com/index.php/2017/10/21/locating-monero-users-via-transaction-broadcasts/
[17]https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
[20]http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf

Revision History

Version Number	Description	Date	Modified By
1.0	Initial Draft	2017-07	IridiumDev
1.10	Complete Rewrite (draft)	2018-02-23	Matthew Therault
1.11	Technical Corrections	2018-02-23	Steve Brush
1.12	Edit/Proofread/Feedback	2018-03-02	h0h0h0
1.20	Reconstruction and Rewrite (draft)	2018-05-26	h0h0h0
1.21LAUNCH	Font Update, Image Addition	2018-06-21	h0h0h0