Galactum
Registration
Adresse

Galactum

WhitePaper

V 1.0

Introdution

The purpose of this white paper is to present the Galactum digital solution and the associated Galactum project. In no case it should be considered as investment advice.

The Galactum was created to support medical research.
Our association has developed its own currency, based on the Cryptonote protocol.
This currency will allow you to pay on Internet sites and commercial applications.
You will see the world of cryptocurrency otherwise.

Disclaimer

However, as this white paper also relate to the Galactum ICO perspective, a mandatory disclaimer seems appropriate at this stage of the document. Here are a few reminders of what you should consider if you are reading this document

- An investment in the Galactum carries with it significant risk. Prior to participation, carefully consider the potential risks and, to the extent necessary, consult a lawyer, accountant, and/or tax professional to evaluate the risk entailed.

- The crypto currency economy is relatively new and incredibly innovative. Crypto currency could be impacted by regulatory actions, including restrictions on ownership, use, or possession. There is no guarantee that the Galactum purchased will increase in value, provide a return, or will have sufficient adoption and liquidity to enable exchange for other assets.

- All possible future risks related to Galactum and its experimental technology cannot be enumerated here. We do not assume responsibility for any losses that may occur. Please exercise caution with all cryptographic assets and do not invest money that you cannot afford to lose.

- We do not promise any gain or return on investment. You can potentially lose all your money if the market price of Galactum drops to zero.

If you have any question regarding the regulations impact on our project, feel free to contact us at support@galactum.site.

Also note that the current document revision is 1.0 It is given as-is and may be updated at any moment. Nevertheless, there is no risk that a future document update would change the basic meaning of what Galactum is.

Table of contents

ABOUT GALACTUM

Galactum was created in 2019 by two technology enthusiasts. Our association is registered as the French Association (Law 1901) (registration number C79790) in France. Our team is made up of several people around the world. (Decentralization is the asset of our currency, and its team), it allows us to share a vision of the world from many countries, religion, and any sector activity.

Since the beginning of the project, we are working on a solution, allowing us to collect through Cryptonote technology, a means of payment allowing us to make donations worldwide.

An e-commerce project

The Galactum is unique in the market:

- It is affordable, which means that with its price, we have the opportunity to reach a much wider audience, who would not be interested otherwise.

- An online sales platform will allow our customers not to be forced to subscribe to several solutions to benefit from the same level of service. We will connect, seller and buyer within the same platform.

It is fully serviced, as opposed to the self-made model. This means that our customers do not need any technical knowledge to get started and that the learning curve is very easy to overcome.

Galactum’s market and current problems

The Galactum team is currently mainly located in France. By 2020, Galactum will begin to target medical projects for selecting those which will be donated.

When watching Galactum as a whole, digital payments are the heart of its approach.

Today, only one exchange channel exists but later other will open :

- End customers exchange their Glcm * (Galactum) with each other, in order to make payments for their sale and / or service.

- Another channel is expected to open soon, with the opening of the Galactum on crypto-active markets.

- In the course of 2020, we hope to be able to launch our first online sales platform, connecting sellers and buyers to pay their Glcm * (Galactum) purchases in an official way, with all the rules that frame this functionality.

Our vision about Galactum

First of all, when writing a white paper, a fundamental question has to be asked: Why in Galactum do we think we need our own digital coin?

- Because we want to help the poor, in medical wandering or who suffers for lack of treatment;

- Because we like to do things ourselves and are passionate about the technology behind the blockchain concept as a whole;

- Because we like to understand what we are doing at the technical level.

- Because we want to build our own community that will decide future technological improvements of our blockchain (and digital currency of course);

- Because we want to introduce new concepts;

- Because it is a unique opportunity for a new currency, to be able to finance research, through donations, via a protocol that recovers X% of each reward;

The second fundamental question is: what are we going to do with our digital play?

Our vision is to give access to the Galactum ecosystem to every e-commerce platform developer.

- We have defined a road map to achieve this goal (see §The Galactum Roadmap). Here are the few use cases expected at the time of writing this white paper:

- Access the Galactum ecosystem for more information on this topic, go to (http://www.galactum.site/).

- The possibility of acquiring Glcm * (Galactum), by mining our currency at this address (http://pool.galactum.site).

- Of course, this list is not exhaustive and will necessarily be completed over time by other use cases.

The Galactum technology

The Galactum is derived from the CryptoNote project, an open-source technology and 1 concepts for the cryptocurrencies of the future.

Features :

Untraceable payments :

Galactum payments are untraceable thanks to a completely anonymous payment schema implementing a ring signature technology. 2

This ring signature technology is a more sophisticated scheme of transaction verification that implies several different public keys. In comparison, traditional transaction verification involves only the public key of the signer (the one who initiate the transaction).

In the ring signature algorithm, groups of individuals with their own key pair are established for each transaction. A member of a group can sign a transaction with his own secret key, but the public keys of all the others members of his group are required to validate the transaction. This ring signature algorithm is a one-way process and cannot be reversed. That way, it is technically impossible to determine who the initial signer was among all the individuals of the group.

Unlikeable transactions Receivers have multiple unique one-time addresses derived from their single public key which makes it impossible to cross-link payments.

With this principle, the CryptoNote algorithm solved the fact that everyone was able to check all the incoming transactions (and thus the resulting balance) of a given public address.

Thanks to a change in the Diffie-Hellman exchange protocol, the sender now uses the receiver's public address and his own random data to compute a unique one-time key for the payment. The sender can produce only the public part of the key, whereas only the receiver can compute the private part.

The CryptoNote website is available at https://cryptonote.org and the whitepaper is downloadable from 1 https://cryptonote.org/whitepaper.pdf The features section is mainly extracted from the CryptoNote implementation details exposed at https://2 cryptonote.org/inside

The receiver is the only one who can release the funds after the transaction is committed. He only needs to perform a single-formula check involving his private key on each transaction to establish if it belongs to him. No third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.

Double-spending proof :

In the CrytpoNote implementation of the ring signature algorithm, a linkability feature has been added to restrict a signer to create more than one ring signature using the same private key, which would indicate a double-spending attempt.

To support linkability, a special marker called a key image has been added to every signature. The key image is the value of a cryptographic one-way function of the secret key. Onewayness means that given only the key image it is impossible to recover the private key. On the other hand, it is computationally impossible to find a collision (two different private keys, which have the same image). Using any formula, except for the specified one, will result in an unverifiable signature. All things considered, the key image is unavoidable, unambiguous and yet an anonymous marker of the private key.

All users keep the list of the used key images (compared with the history of all valid transactions it requires an insignificant amount of storage) and immediately reject any new ring signature with a duplicate key image. It will not identify the misbehaving user, but it does prevent any double-spending attempts, caused by malicious intentions or software errors.

Blockchain analysis resistance :

The unique one-time addresses and the ring signature make the whole blockchain resistant to analysis.

Since every ring signature produces ambiguity, there are billions of possible graphs linking addresses with transactions. Moreover, every next transaction increases the entropy of the whole blockchain and creates additional obstacles for an analyst.

Egalitarian proof of work :

The proof of work mechanism is actually a voting system. Users vote for the right order of the transactions, for enabling new features in the protocol and for the honest money supply distribution. Therefore, it is important that during the voting process all participants have equal voting rights. CryptoNote brings the equality with an egalitarian proof-of-work pricing function, which is perfectly suitable for ordinary PCs.

Adaptive limits :

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the network to develop on its own.

CryptoNote has the following parameters which adjust automatically for each new block:

- Difficulty. The general idea of the algorithm is to sum all the work that nodes performed during the last 720 blocks and divide it by the time they have spent to accomplish it. The measure of the work is the corresponding difficulty value for each of the blocks. The time is calculated as follows: sort all the 720 timestamps and cut off 20% of the outliers. The range of the rest 600 values is the time which was spent about 80% of the corresponding blocks.
- Max block size. Let MN be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is 2*MN. It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary. Transaction size does not need to be explicitly limited. It is bounded by the size of the block.

Services

Wallets

As indicated in our roadmap (see §The Galactum Roadmap), desktop portfolios with a graphical interface have been published to facilitate decentralization.
The command line portfolio is of course available on our GitHub at (https://github.com/Sab-Barsoom/Galactum/releases)

Exchanges

As outlined in our roadmap (see the "The Galactum Roadmap" section), an integrated trading platform will be published end 2019 to early 2020 to allow Galactum trading. In the meantime, we will work very hard to bring the Galactum to several popular public exchanges.

The Galactum initial distribution

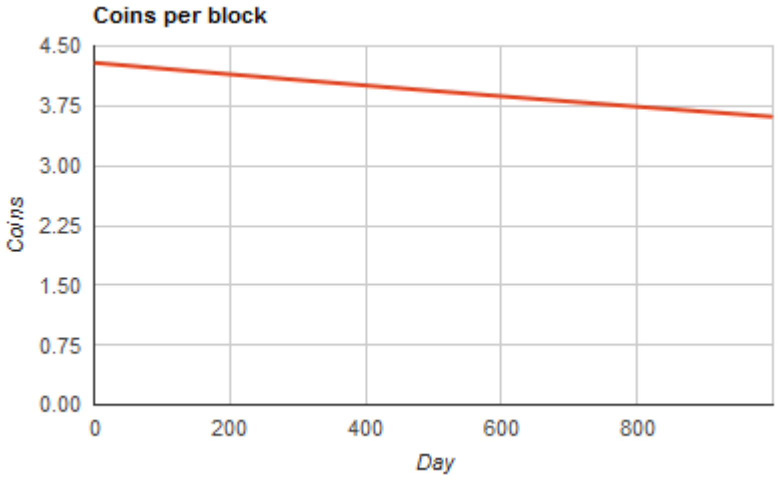
From the beginning, it was planned to give the Galactum a large but limited supply. A total of 18,000,000 Galactum will be issued.

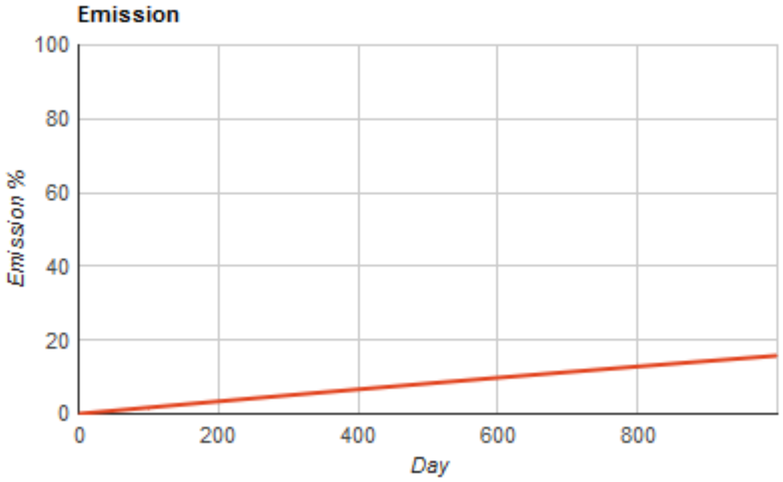
A relatively slow emission curve has also been chosen voluntarily.

The Galactum show started on 31/05/2019.

Emission speed factor = 22

Coins Decimal point = 12





The Galactum Airdrop

It takes place during the ten months following the official launch of the project (June 2019 to the end of March 2020).

During these drops, each participant who has made available, his time and skills to perform services, in order to make known the Galactum will be granted a paiement in Glcm.

Promoting the Galactum to the community or referencing it on different platforms or making him alive will be paid by referencing operated, within the limit of 1 subject per platform;

Of course, the diffusion of Galactum is limited. Anyone trying to play with the system will have their participation canceled and no reward will be paid.

Contact

Feel free to contact us for any question / suggestion or to get involved in the Galactum project.

Email :	support@galactum.site
Discord	https://discord.gg/Jsc9qdR
Bitcointalk	https://bitcointalk.org/index.php?topic=5183455.0
Website	http://www.galactum.site/
Telegram	https://t.me/galactum