# FoldingCoin White Paper

Mine Medicine, Not Hashes





Robert Ross - Founder
rross@foldingcoin.net

James Sewell - Lead Developer
jsewell@foldingcoin.net

## FoldingCoin Mission Statement

FoldingCoin Inc.[1] looks to harness computational power used in alternative cryptocurrency blockchains to be better used for medical and scientific projects with goals of solving world problems. In doing so, FoldingCoin Inc. looks to compensate participants with cryptocurrencies built on Counterparty.

## Goals of FoldingCoin Inc.

FoldingCoin Inc. was created with the intent to solve current issues dealing with cryptocurrency mining and distributed computing platforms.

## FoldingCoin Inc. Summary

- FoldingCoin Inc. is an Indiana Not-For-Profit Corporation[2] formed under the Indiana Nonprofit Corporation Act of 1991.
- FoldingCoin Inc. distributes cryptocurrencies (tokens) to affiliated participants on the Stanford University Folding@home network. The tokens are awarded proportionally, according to that participant's Folding@home credits.
- FoldingCoin Inc. looks to redirect what some consider to be wasted computational power from alternative cryptocurrencies to distributed computing platforms, and to incentivize those who compute on non-profit distributed computing platforms to encourage continued support.
- FoldingCoin Inc. has measures in place to allow all interested participants to have a say in future developments, and to vote on specific proposals for change.

---

[1] FoldingCoin Inc. http://foldingcoin.net/
[2] Indiana Non Profit https://secure.in.gov/sos/online_corps/name_search_results.aspx?search_name=foldingcoin&search_type=exact&client_id=&submit.x=0&submit.y=0&search_mode=search

# Table of Contents

# 1.0.0 - Required components of FoldingCoin

## 1.1.0 - Cryptocurrency Mining

Cryptocurrencies are digital systems (protocols) for exchanging value between participants on a decentralized computer network. Bitcoin (BTC)[3] is the most famous and widely adopted cryptocurrency. Most cryptocurrencies use hard-to-solve cryptographic puzzles called “Proof of Work” to secure the operation of the network. The process of verifying the cryptographic solutions is commonly referred to as “mining”.

Bitcoin introduced a “reward” system, where the miner who solves a block is awarded a small amount of the cryptocurrency. This reward compensates the miner for contributing their hardware and electricity to the mining network. The solution of a block is a vital operation to allow distributed consensus and add the block to the blockchain.

In the early days, one could mine a decent amount of Bitcoin blocks on standard computing hardware, most notably CPUs (central processing units) and GPUs (graphics processing unit). Bitcoin uses the SHA256 hashing algorithm for Proof of Work.

In 2013, ASIC (Application Specific Integrated Circuit) mining hardware, specializing in SHA256, began to dominate and Bitcoin mining was no longer profitable on general purpose computers. It was around this time that hundreds of alternative cryptocurrencies released blockchains to try to compete with Bitcoin. Many of these “Altcoins” used standard computing hardware from miners that had previously mined Bitcoin before the ASICs took over. Many used the Scrypt algorithm instead of SHA256. This was to allow the continued use of general purpose computers to mine the Scrypt coins as ASICs could only mine SHA256 coins. Many former Bitcoin miners moved to Scrypt coins. In early 2014, Scrypt ASICs appeared, and once again mining was no longer feasible to the non-specialist miner.

The phrase “standard hardware” refers to CPUs and GPUs found in everyday consumer and corporate PCs. The energy consumption of standard hardware in comparison to ASIC hardware is not as efficient.

Many believe that altcoins are a problem because of the following reasons:

- The amount of energy used to hash these blockchains is considered by many to be a vast waste of energy
- Most of these coins die off
- These coins can be underdeveloped or become abandoned

[3] Bitcoin - https://bitcoin.org/en/

- End up being a scam coin
- Traded as a “pump and dump” coin
- Bring no new great innovations to Bitcoin itself

## 1.2.0 - Scientific Distributed Computing

Cryptocurrency mining was not the first application for distributed computing. The Internet emerged as a consumer phenomenon in the late 1990’s and early 2000’s. Soon after, scientific investigators found applications for distributing massively parallel computing jobs to individual consumers. Consumers could install software provided by the scientific investigator on to their own computer and leave the machine powered on even when not actively using it. The scientific investigators would use the leftover computing cycles to assist in solving their scientific problems.

An early example of such a system was Distributed.net[4] founded in 1997. The initial problem they investigated was the mathematical principle of the “Golomb ruler”. Once the 27 and 28 mark Golomb rulers were solved, they moved on to trying to break the RC5-72 encryption standard. They remain active and expect to take 200 years to exhaust the RC5-72 key space.

In addition to Distributed.net, two other popular platforms have dominated the grid computing and distributed computing communities: Berkley’s BOINC[5] and Stanford’s Folding@home[6]. These systems have gained mass adoption in the little under two decades they have been operating. Between them, these networks have hundreds of thousands of participants, combined contributing millions of computational FLOPS. Today it can be seen that these projects are still larger than most supercomputers and have an immense combined power of somewhere between 80-100 PetaFLOPS[7] (the largest single supercomputer is 33 PetaFLOPS and number 2 is 17 PetaFLOPS[8])

## 1.3.0 - Folding@home

Stanford University started the Folding@home project (FAH) in October 2000. The project runs computational algorithms, to simulate the way protein molecules fold in the body. Protein folding is central to healthy biological processes. Cancer and Alzheimer’s (among others) are well known medical conditions that arise when proteins misfold. Scientists and medical researchers alike investigate why the proteins fail to fold properly and how medicines can be designed to correct the process. Stanford provides the data output from the FAH program to these researchers in order to help understand how to solve the misfold issues.

Simulated protein folding is a problem that can be solved by many computers working in parallel. When a donor joins the FAH project, they register an account, install a program, and FAH begins downloading “work units” to their computer. Work units are “bite sized” protein folding problems that the FAH researchers want to learn more about. From this research many

---

[4] Distributed.net http://www.distributed.net/Main_Page
[5] Berkley’s BOINC http://boinc.berkeley.edu/
[6] Stanford’s Folding@home http://folding.stanford.edu/home/
[7] Distributed Computing Power http://en.wikipedia.org/wiki/List_of_distributed_computing_projects
[8] Most Powerful Supercomputers http://www.top500.org/lists/2014/06/

scientific papers have been written and can be found here[9].

As a donor finishes a folding problem and submits the solution to FAH's server, they are assigned more work units. Modern day computers have CPU speed, memory capacity, and graphics performance that would have been hard to imagine years ago. The FAH software takes advantage of all this newly developed hardware.

The faster one's computer completes work units, the more "credits" one can earn. FAH's public statistics system[10] keeps "score" of all work submitted and credits earned by all donors. But these credits carry no value themselves, beyond "bragging rights".

### 1.4.0 - Counterparty and User Created Assets

In 2014, many extensions to the Bitcoin protocol emerged, commonly referred to as "Bitcoin 2.0" systems. Bitcoin 2.0 systems use the distributed blockchain technology pioneered by Bitcoin to extend the network in novel ways that were not envisioned by Satoshi Nakamoto and the early Bitcoin Core developers.

Counterparty[11] is an example of a Bitcoin 2.0 system that allows users to create their own assets, along with a complete suite of additional financial tools, within the Bitcoin blockchain. A user or project with a unique value proposition can use Counterparty's open source technology to create a cryptocurrency asset. The user created assets are often generically referred to as "tokens" or simply "assets". A cryptocurrency project can use and distribute the tokens in support of their value proposition in nearly any way they see fit.

Since Counterparty is built inside of the Bitcoin blockchain, it requires a Bitcoin transaction for all actions taken with these assets. This is accomplished by inputting the data from these assets in the 140 bytes of unused data that each Bitcoin transaction allows.

### 1.5.0 - LetsTalkBitcoin! Asset Distributor

The media outlet "LetsTalkBitcoin!"[12] created a distribution system that allows someone to distribute a mass amount of these tokens by simply uploading all the recipient addresses and total amount of tokens they are to receive in a CSV format. Then the distribution server automatically sends the allocated amount of the token to the address in which is in the same row as the amount.

## 2.0.0 - Genesis of FoldingCoin Inc.

By July 2014, a group of miners were looking for ways to use their legacy mining hardware for useful purposes, while staying part of the cryptocurrency movement at the same time. This became FoldingCoin Inc.

FoldingCoin Inc. created an asset with a "Proof of Fold" concept to verify contributed computational power. Participants contribute their cycles to medical research on the

---

[9] FAH White Papers http://folding.stanford.edu/home/papers
[10] FAH Team and Donor Stats http://fah-web.stanford.edu/cgi-bin/main.py?qtype=userstats
[11] Counterparty http://counterparty.io/
[12] LetsTalkBitcoin! https://letstalkbitcoin.com/

Folding@home platform instead of a “Proof of Work” or “Proof of Stake” algorithm on a traditional Altcoin blockchain. This makes the energy to receive the token go towards something more meaningful than an alternative blockchain to Bitcoin’s blockchain. Thus the power is not considered wasted, as it goes towards medical research.

Since Counterparty assets share the Bitcoin blockchain, this allows the legacy mining equipment from Altcoin mining to be redirected towards medical research, since the Bitcoin miners are already covering the security and hashing rate of the Bitcoin blockchain.

## 2.1.0 - Choosing the right distributed computing platform

FoldingCoin Inc. researched many scientific distributed computing projects that would allow for the use of the legacy mining equipment, and pros and cons were found for each. They wanted to find a distributed computing platform that worked best with the mining hardware that was common amongst a large majority of the mining community. Many factors had to be considered:

- **Common hardware:** The hardware most commonly used for Bitcoin and Altcoin mining was AMD/ATI GPUs. AMD/ATI GPUs outperform Nvidia GPUs when it comes to SHA256 and Scrypt hashing. Folding@home (FAH) also performs very well on AMD hardware.
- **Easy:** Ease of setup for the general computer user was also evaluated. FAH was the most polished here creating a simple “download and go” program that runs in the background of a PC with simple to use settings.
- **Large user base:** Besides the Bitcoin Network, FAH is the largest distributed computing platform in the world, harnessing nearly 50 PetaFLOPS of computational power. With more users on the FAH platform, it makes it easier to gain awareness about the new token reward system.
- **Strong development team:** FoldingCoin wanted to find a platform that had a solid development team and mission. FAH is superior when it comes to overall production and security. Since FAH is a stand alone project on the platform, the developers of FAH spend all their time focusing on bettering the FAH platform, without the worries of developing and maintaining other distributed computing projects. FAH has also gone to great lengths to provide solid security of download and uploads of the protein data files. FAH only interacts with a special file extension compiled by the project and no other files or data on a personal computer[13].
- **Non Profit:**The platform chosen must be a non profit platform with goals of bettering humanity. Without the platform being a non profit, this would create issues of building profit on top of an already profitable platform. FAH is a 501(c)3[14] company with all the data available to medical and scientific researchers upon request.

FoldingCoin decided to direct their efforts towards integrating with Folding@home.

## 2.2.0 - Already existent “cause” coins

[13] FAH Security Measrues https://folding.stanford.edu/home/faq/#ntoc45
[14] Folding@home 501(c)3 https://folding.stanford.edu/home/donate/

There are also some existing cryptocurrency projects such as CureCoin and GridCoin that had involvement in scientific distributed computing, but these run their own separate blockchains. FoldingCoin decided that with the advances in Bitcoin 2.0 systems, there was no longer a compelling need for a separate blockchain. A separate blockchain did not contribute anything novel to the project, but rather would require more focus for the developers. They would have to put time and resources into the creation, hash rate, and security of a brand new blockchain and wallet interface. This would take away time and resources from developing uses, applications, economy, and adoption for the coin.

## 2.3.0 - Creation of FoldingCoin

FoldingCoin is a cause coin built on Counterparty. Distributed on a schedule, FLDC is given to those that donate cycles to Folding@home based on their individual contributions.

An initial announcement forum and call out for developers to join the team was posted in early July 2014 in a forum post at LetsTalkBitcoin! which can be found here[15].

The ease of both creating Counterparty assets and accessing the FAH public stats allowed for a manually computed proof of concept. The first weekly distribution of “FLDC” tokens was on July 14, 2014, to eight folders paying from a folding time period of July 6th - July 13th.

The project gained traction and the proof of concept showed this would be a viable venture. The entity that would soon become FoldingCoin Inc. set up a hosting account with a commercial provider that would allow execution of custom PHP code. The distribution method that had been manually calculated was reduced to a set of PHP scripts that could be run from a cron job. Also with the addition of the “LetsTalkBitcoin!” asset distributor, FLDC could be automatically distributed to any amount of Counterwallet addresses without having to manually send them out one at a time. With the combination of these two features, FoldingCoin Inc. was able to start paying out FLDC to the donors on a daily basis and began this on August 11th 2014.

### 2.3.1 - FoldingCoin (FLDC) asset details

*Only 1 billion tokens will ever be created*

This is a hard cap. The asset has been locked and there is no way for anyone to ever issue more of them.

*Tokens will be distributed according to a half-life schedule*

The Half Life will proceed as follows:

- Once 500,000,000 FLDC are distributed, daily distribution becomes 250,000 FLDC
- Once 750,000,000 FLDC are distributed, daily distribution becomes 125,000 FLDC
- Once 875,000,000 FLDC are distributed, daily distribution becomes 62,500 FLDC
- And so on. This halving occurs every 1,000 days

*There are no fees*

There will be no service fees. Stats on who was paid will be updated to the website regularly to keep the issuer in check and to insure that all payments have been received.

[15] FoldingCoin Inc. Ann Forum http://letstalkbitcoin.com/forum/post/asic-proof-altcoin-on-counterparty

*Won't ASICs just attack this?*

In order for an ASIC to contribute folding power to earn FLDC, one would have to get a hold of an Anton SuperComputer which is an ASIC specifically for protein folding and this doesn't seem possible anytime soon. And if it was to be created, this would help bring more computational power towards FAH so can only be a good thing.

### 2.3.2 - FoldingCoin Distribution Calculator

As mentioned above, FoldingCoin Inc. uses PHP code running on a commercial hosting provider to calculate how many FLDC tokens to award to each folder. The code runs once a day and awards a total of 500,000 FLDC tokens per day, proportionally to FAH credits earned by each folder in the 24 hour period since the previous day's snapshot. Once the half life occurs on March 23rd, 2017 the daily distribution amount will become 250,000 FLDC per day. Then every following 1,000 days this amount will once again be cut in half for the daily distribution.

*Folding@home Public Statistics*

Folding@home (FAH) provides a text file[16] listing every folder on the network and how many credits they have folded at the moment text file was produced. This file is placed on FAH's public website for anyone to download, and is updated once an hour.

*Daily Snapshot*

Once a day, FoldingCoin Inc.'s snapshot code downloads the FAH daily user summary text file and searches line by line to find those folders who have set up their folding software according to the FoldingCoin Inc. instructions

- In the initial release of FLDC, anyone who wanted to get the tokens had to join FAH team 226728 and set their FAH user name to their Counterwallet Bitcoin public address. This scheme worked very well for the initial roll out and is still fully supported to the present day for the original Folders. It will not be advertised heavily as it is not recommended and further developed code has replaced this model.
- Responding to feedback from existing folders on FAH, in October 2014 a method was devised where a FAH user would not have to change teams, and could have a more friendly identifier than just a Bitcoin address. The new scheme works with any FAH team. A folder indicates the address to award their tokens by setting their FAH software to:
  **username_FLDC_CounterwalletAddress**
  The snapshot code looks for "_FLDC_" and uses this to determine FLDC folders. Here is an example of a real Folder:
  **PookTwo_FLDC_16muW9htJAYrrXrKN8BwWTmT6cgXscXDzJ**
- Regardless of which scheme the folder used, all affiliated folders get their up-to-date FAH credit quantity written to that day's FLDC "snapshot" in the MySQL database.

*Calculation of Tokens to Award*

After the snapshot, a separate process runs to calculate token award amounts:

- Each folder in the current awarding period's snapshot is read.

[16] FAH Donor Text File http://fah-web.stanford.edu/daily_user_summary.txt.bz2

- The code determines if the folder's address is a valid Bitcoin wallet address. If their Bitcoin address is not valid, there is no point in including the folder in any further calculations that awarding period. There would be no way to send them their FLDC tokens. These invalid FAH credits are simply disregarded.
- For each valid folder, their credit count in the previous awarding period's snapshot is determined, and subtracted from the current awarding period's credit count. This results in a "delta". The delta shows how many FAH credits have been earned by that folder in just the current awarding period.
- The total number of FAH credits earned that awarding period by every folder with a valid FLDC address is computed by adding together all the deltas. Since 500,000 FLDC tokens are currently distributed each awarding period, it can be determined how many FLDC are awarded per FAH credit, by dividing 500,000 by that awarding period's total number of earned credits.
- The list of valid folders is then read and that folder's delta is multiplied by that awarding period's FLDC amount per FAH credit, and this determines how many FLDC tokens go to each address.
- The awarding period's list of valid folder addresses and corresponding FLDC token amounts is rendered as CSV formatted data suitable for entry into the LTB asset distributor and emailed to the FLDC developers.
- Finally, the same data is formatted appropriately for statistical inclusion on the website.
- All of this calculated data is available on the FoldingCoin Inc. distribution summary[17] webpage.
- All mass distribution addresses[18] can also be found on the website with each individual Bitcoin transaction associated with each payout

*Let's Talk Bitcoin Asset Distributor*

The FLDC team has leveraged "LetsTalkBitcoin!" (LTB) from the start. LTB has been great for building communities in the crypto space and this is where the FLDC developer met each other.

LTB was an early adopter of Counterparty for their LTBCoin member reward system. The LTB team coded an automated system for distributing Counterparty tokens to individual wallet addresses.

LTB has authorized FoldingCoin Inc. to use their automated distributor. This was a great improvement over the manual transactions that were done during the proof of concept stage. The way that the LTB distributor works is as follows:

- The title of the distribution is submitted, FLDC uses the method "0300 EST FLDC Payout 2/16/15" but this title can be anything
- The Counterparty asset that is to be distributed is entered.
- A CSV file can be imported containing the receiving Counterwallet addresses in the first column and the amount to receive in the second column OR it is pasted into the entire list with each address having a comma after it then the amount of asset it should receive

[17] FLDC Daily Summaries http://stats.foldingcoin.net/platformReports/FLDC/
[18] FLDC Distribution Payouts http://foldingcoin.net/distrihttp://foldingcoin.net/distribution/bution/

putting each address on its own independent line
- The Asset Distributor then tallies up how much of the selected token must be sent to a specific newly generated BTC address and the amount of BTC that must be sent to that same address to distribute all the assets
- Once the Asset distributor has these funds it will automatically distribute to the addresses and amount of the selected asset allocated to them
- Every asset distribution address that FoldingCoin Inc. has sent out since the beginning, can be found on the distribution webpage[19].

### 2.3.3 - Merged Folding

The FoldingCoin Inc. team members have received overtures from other Altcoins asking how it was done and how they can follow the same model for their coin. Other Altcoins have had concerns over maintaining their own blockchain, gaining adoption, gaining trust in the community, and the overall concern about the vast amount of energy that is put into mining rather than something more productive. Many have wondered if “merged folding” is a possibility.

Since Folding@home tallies up statistics (credits) based on the amount of computational power each individual participant contributes, FoldingCoin has the ability to incorporate multiple coins into the open sourced distribution calculator[20] based on individual missions of the respective coin. These include:

- Altcoins looking to develop a new coin for a particular service but not wishing to develop their own unique blockchain could use this methodology to distribute their coins to their participants.
- Since FoldingCoin only distributed coins to participants of the Folding@home project, this leaves many other distributed computing projects without a token to be used as an incentive. One could be created and distributed on FoldingCoin Inc.’s platform to entice participants.
- There are a number of existing Altcoins that have individual blockchains with development teams having a hard time maintaining their own blockchain with small development teams. These coins had been released before Counterparty had been released. FoldingCoin can work with these existing coins to move their coins over to the Counterparty platform and get rid of their existing blockchains so the coins development team can focus more on the economy and use cases for their coins.

FoldingCoin has developed a system where new tokens could have their participants enter a different prefix to their donor name to start receiving the new respective tokens in addition to FLDC for their folding efforts. Still following the same distribution methodology from the above section, FLDC participants can now earn the additional tokens[21] by simply changing their donor names using the following format:

- Folders wishing to receive only FLDC should use the prefix

---

[19] FLDC Asset Distribution addresses http://foldingcoin.net/distribution/
[20] FoldingCoin Inc Distribution Calculator https://github.com/FoldingCoinNet
[21] Merged Folding Tokens http://foldingcoin.net/alttokens/

**username_FLDC_CounterwalletAddress**
example from a real Folder:
**PookTwo_FLDC_16muW9htJAYrrXrKN8BwWTmT6cgXscXDzJ**

- Folders wishing to receive only FLDC and the selected tokens use the prefix **username_TOKENSYMBOL_CounterwalletAddress**
  example from a real Folder:
  **PookTwo_SCOTCOIN_16muW9htJAYrrXrKN8BwWTmT6cgXscXDzJ**
- Folders wishing to receive every token on the platform should use the prefix **username_ALL_CounterwalletAddress**
  example from a real Folder:
  **PookTwo_ALL_16muW9htJAYrrXrKN8BwWTmT6cgXscXDzJ**

With more tokens being added to the FoldingCoin Inc. distribution family, more adaption is gained for Folding@home, FLDC, Counterparty, and the respective token, all at the same time. Tokens added in this way will be advertised as a collaboration effort on FoldingCoin Inc.'s part, but will still be developed and run separately from FoldingCoin Inc.

Each token will have its own distribution methodology. What that means that the tokens' developers will choose when and how much to distribute. They will also have their own unique way of cutting that distribution amount down should they desire. FoldingCoin Inc. is setup to allow anywhere between daily to monthly distributions and all variations in between.

*Statistics and Calculations*
The calculations for Merged Folding will take place every day for each respective TOKEN. There are basically going to be 2 different kinds of calculations that FoldingCoin Inc. will calculate:

1. **_FLDC_** - This calculation will be for all the Folders that have this prefix along with any other prefixes in their names. This is the overall FAH credits amongst every Folder on the FoldingCoin Inc. platform regardless of prefix. Those that have the extension _FLDC_ will only receive FLDC though.
2. **_TOKEN_** - There will be a separate calculation for each TOKEN prefix on the Merged Folding platform. This calculation will tabulate all the FAH credits from the independent TOKEN prefix along with the _ALL_ prefix names. This will show the amount of FAH that is going towards that particular TOKENs FAH power.

*TOKEN Distribution*
FLDC will be distributed by FoldingCoin Inc. daily still and we allow the TOKENs built on our platform to decide how often they wish to to do their distributions. This can be done daily, weekly, or monthly. It could even be done with some combination in between if needed. Once the distribution is decided by the TOKEN development team, the TOKENs admin will be sent an email by FoldingCoin Inc. giving them a Bitcoin address that they must send X amount of the TOKEN and BTC required for transaction cost in order for the distribution to be pushed through on the designated time that the TOKEN has discussed. Once the TOKENs team send the funds off, the distribution address will automatically send the funds to the proper Counterwallet

address.

- If the distribution is daily, then the payouts will pay for the amount of FAH work that was put into the previous day of work.
- If the distribution is weekly, than the previous week of folding will be added up collectively. So if Folder X earned 20 TOKENs on 4 independent days and earned 10 TOKENs on 3 independent days throughout the week, then they would receive 110 TOKENs on the weekly distribution
- If the distribution is monthy, than the previous month of folding will be added up collectively. So if Folder X earned 1 TOKEN on 15 independent days, and 2 TOKENs on the other 15 independent days throughout the month, then they would receive 45 TOKENs on the monthly distribution

*Disclaimer*
*FoldingCoin Inc. will only assist the respective tokens in the calculation of the respective token payouts, provide the distribution platform, and provide assistance to new Folders on the platform including setup and general inquires. FoldingCoin Inc. does not charge any amount financially to any tokens development team on the platform for the provided services. FoldingCoin Inc. is not responsible for any actions taken by the respective tokens development team or payment issues regarding the respective token. You will still receive FLDC from the staff but any discrepancies with other token payments should be taken up with those token developers and not FoldingCoin Inc, unless the discrepancy involves a lack of FoldingCoin Inc. providing the respective token with a distribution address. This would then fall under FoldingCoin Incs. responsibilities. FoldingCoin Inc. reserves the right to remove any coin from this list due to lack of development, distribution payouts, or anything done in a manner that could hurt the image of FoldingCoin Inc. Should a token be removed in this way, FoldingCoin Inc. will still continue to distribute FLDC to usernames using the removed token by simply replacing the respective tokens COINSYMBOL function with the ALL function in the database. This will still enable you to receive future tokens as well as FLDC.*

### 2.3.5 - Token Controlled Access

FoldingCoin Inc. leverages the Let's Talk Bitcoin (LTB) community-building site extensively. Since LTB launched their Token Controlled Access (TCA) platform, there is an additional feature that allows for the creation of a forum page that only one holding a particular token can access.

Using TCA, FoldingCoin Inc. has private forums which only holders of FLDC can access. This allows us to have conversations that are limited to those who are invested in FLDC. The conversations stay more on topic and will have less trolls or side conversations about things unrelated to FLDC and the mission at hand.

FoldingCoin Inc. has set up two TCA forums on LTB, one for general folder discussion and one geared specifically for technical support, FAH, hardware, and scientific discussions.

FoldingCoin Inc. is still very active in all public forums including the ANN thread on

bitcointalk.org[22], this just gives an opportunity for the holders of FLDC to have a secure place to talk amongst the rest of the community.

# 3.0.0 - Counterparty Assets VS. Traditional Altcoins

Counterparty assets have significant differences from traditional Altcoins. FoldingCoin Inc. believes that the pros significantly outweigh the cons, but wishes to be transparent about the various feedback that was given. The following sections will go over arguments for both sides and rebuttals for each one.

## 3.1.0 - Benefits of Counterparty

- BTC miners hash the blocks for the transactions. This provides a strong foundation of security, based on cryptographic computations on the largest distributed computing platform currently in operation.
    - REBUTTAL - Since Counterparty is using the Bitcoin blockchain, no new innovative ideas such as lower transaction times are incorporated in the tokens. Unless Bitcoin is updated to address potential concerns, Counterparty runs just as Bitcoin currently does.
- Asset issuance can be locked by the Counterparty protocol ensuring that even the asset owner can't introduce more of the token into the market. FLDC was created as a locked asset[23].
    - REBUTTAL - Even with the "locked" asset feature, it is still possible for the owner of the token to take control with bad intentions to steal the undistributed tokens once they become valuable.
- As Bitcoin and Counterparty developers innovate, assets evolve with them. Since Counterparty is open source, developers throughout the community create new and innovative ideas to be applied to Counterparty. When Counterparty or outside developers create applications for Counterparty, all assets are compatible automatically. Most Altcoins have to develop their own apps and features since they have a separate blockchain. Many Altcoins do not have a high enough interest in the overall crypto community for outside developers to create applications for them.
    - REBUTTAL - Many Altcoins that introduce new innovative ideas like anonymous transactions have gained strong support from outside developers.
- No direct mining is required for Counterparty assets. Token creation and transfer can be verified by third party sites such as "blockscan.com" yet still verified by the BTC Miners. For the FLDC asset, this is available at Blockscan.com[24]
    - REBUTTAL - Although no resources are used to hash a blockchain, the verification system depends on the security and coding efforts put forth by the Counterparty team. Since Counterparty is an application, it could have a potential bug that could affect the Counterparty network.
- There is no exposure to a 51% attack unless it happens to the Bitcoin network itself.

---

[22] FoldingCoin ANN thread https://bitcointalk.org/index.php?topic=781352.0
[23] FLDC Locked Asset http://blockscan.com/assetInfo/FLDC
[24] Blockscan.com FLDC Info http://blockscan.com/assetInfo/FLDC

    - REBUTTAL - Some new Altcoins coming out have implemented a Proof of Stake concept in which the attacker would need 51% of the total coins in existence in order to potentially harm the network. This is much more unlikely than simply having 51% of the total mining power of a network in a lot of cases.
- Counterparty assets automatically get security and GUI updates from the strong Bitcoin and Counterparty developers, due to the common Bitcoin blockchain. Due to this, the asset owner can focus on adoption, distribution, applications, and economy of the coin, and not software development of the blockchain and wallet itself.
    - REBUTTAL - This means that each Counterparty Asset is depenant upon third parties for updates.

## 3.2.0 - Benefits of Traditional Altcoins

- Every asset payment to a recipient from Counterparty assets requires 0.00006 BTC in order to be included on the Blockchain when using the LTB asset distributor for distributing to multiple addresses. If sending a single transaction in Counterwallet, it will cost the current miner fee in addition to 0.000078 BTC. With large numbers of recipients, the BTC costs could be an obstacle.
    - REBUTTAL - That fee could potentially be lowered depending on Counterparty's willingness to change their code. It could also depend on the blockchain accepting micro transactions. The current fear is that miners would reject a satoshi transaction if Counterparty assets only get sent in a single satoshi. As Bitcoin gains value the transaction fees will naturally become lowered.
- Assets on the Counterparty network may be considered "fully pre-mined" since a decentralized blockchain is not continuing to issue new tokens upon block creation. Non-locked assets can have more tokens created at the discretion of the asset owner, instead of creating and locking all tokens at once. This causes the issue of potential mass creation of tokens once the token obtains real value.
    - REBUTTAL - With Counterparty there is no current way of doing decentralized asset creation and issuance. Although you lose the benefit of token creation from hashing a blockchain, you gain the fact that the blockchain is not developed by a underfunded dev team, but rather developed by two highly funded projects being the Counterparty platform and the Bitcoin network.
- The undistributed tokens are in control of the development team. This causes the following concerns:
    - If the development team decides to use the undistributed funds for inappropriate purposes, the option is there for them to do so.
        - REBUTTAL - FoldingCoin Inc. is fully compliant with US law and has incorporated as an Indiana non-profit company. This imposes certain accountability obligations on the organization. The sole beneficiary of all assets if there is ever a dissolution is Stanford University's Folding@home project.

- The undistributed tokens are only as secure as the development team makes them. If the development team lacks in security of the private keys, the funds could be hacked.
    - REBUTTAL - FoldingCoin Inc. takes security of the undistributed tokens very seriously. The team has all but two weeks worth of distribution in a paper wallet and changes that paper wallet once every two weeks once another two weeks worth of funds are needed. The team has the FLDC funds to cover the amount of FLDC that could potentially be stolen from the distribution address. The creation of the paper wallets is as follows:
        - Ubuntu computer that is “air-gapped” to generate the cold storage
        - USB dummy printer connected via USB only with no network capabilities
        - BIP38 wallet encrypted
    - In case of the issue if one dev is unavailable in any way, comodo secured encrypted emails of the BIP38 private keys are sent to the main developers. The password to the key is only communicated via voice call so that way even IF the email is unsecured, only the trusted Devs have the password to unlock the wallet.
    - These steps will be changed to Multisig addresses once a board of directors is established for FoldingCoin Inc. requiring half of directors to sign off on distributions.
- The coin must be distributed by the dev team. Should the dev team lose interest in continuing the project, the token could die.
    - REBUTTAL - By the end of the calendar year the aim is to establish a board of directors who are dedicated to the mission. It is not the aim to just select random developers from the internet either. Medical professionals are also needed on this board that understand protein folding and see the value in something like FoldingCoin Inc. to be in existence. This is one of the main reasons as to why Foldingcoin Inc. wished to incorporate. Now that it is an incorporated non profit, it now has some accountability that has been added to it.
- Automating the distribution must still be done partially done manually. With applications like the LTB distribution system, only one transaction of the total amount of tokens to be distributed needs to be sent to this address, then the server sends the appropriate amount of tokens to the designated addresses, but a dev must still be responsible for sending the first transaction to the distribution server.
    - REBUTTAL - This gives FoldingCoin Inc. the chance to give a second look before distributing the funds out to the donors. Should any miscalculations be there, FoldingCoin Inc. has the ability to correct the mistakes before it is sent out.

## 4.0.0 - Project Value and Global Benefits

### 4.1.0 - Appeal to the community

Cryptocurrency mining, as well as Scientific Grid Computing, are both great measures of user-contributed computing power.

Many Bitcoin evangelists have a problem with all the wasted energy that has gone into mining for Altcoins. The trouble with these Altcoins is that many are just a “pump and dump” coin that retains no value in the end. Coins die all the time in this space. But FLDC does productive work instead of securing a blockchain. FLDC is so much more appealing since it represents a real benefit to humanity through medical research.

There are a lot of original Bitcoin miners with a lot of idle GPU and CPU hardware since early 2014 when the ASICs took over the Scrypt mining community. FoldingCoin was developed both as a way to use that hardware productively, and also to provide a boost to the Stanford University Folding@home network.

Adding a cryptocurrency element to FAH attracts gamers, computer enthusiasts, general public and legacy miners, becuase they may not have contributed idle hardware to FAH if all they were getting was points on a leaderboard and a “feel good” outcome. But now that they can get a cryptocurrency token instead of simply gaining folding credits, FAH becomes attractive to a whole new user population since a profit motive has been introduced.

FoldingCoin can reach a large population of the general public by the sweet spot combination of FLDC and FAH. In the social networking outreach, the FoldingCoin team have met many “Non Bitcoiners” who are not comfortable with computers, and who don’t know anything about cryptocurrencies, nor do they care to learn all the intricacies. But they are interested in the project as they can not only use their idle computer for useful medical research, but also generate a valuable asset on the Counterwallet platform which is much easier for the general user to setup than a Qt wallet or Bitcoin Core client. This gets the general public used to the idea of cryptocurrency with a crypto representing something productive that much of the general public can see as valuable.

#### 4.1.1 - Value for crypto

Miners are constantly mining different coins. All sorts of crypto-switching programs can retarget mining equipment every 10 minutes at the most profitable coin. Then instant sell outs for bitcoin occur as the miners just want an immediate profit. This is not a system in which a coin can become established. Many miners don't even know what they are mining the majority of the time. Since folding is on a different platform than mining and requires FLOPS not hashes, it is very hard to switch back and forth between the two. Also the FAH client is only partially open sourced, so coding something that would make the FAH client stop, so mining could begin, is currently impractical for the average Miner.

#### 4.1.2 - Value in earning TOKENS as a bonus

Coins and tokens can have a hard time in gaining mining adoption as many are not worth much, maybe only a satoshi or two. Few miners will mine something that does not provide an immediate return, as most are in it for the profit and not necessarily the coin itself. Being on the

FoldingCoin Inc. Merged Folding platform allows multiple tokens to distribute to an already established folding community to receive its tokens. And should the token fail, the folders will not mind, because they are still receiving FLDC and other future assets by folding.

### 4.1.3 - Value for Miners

Receiving more than one coin is a dream come true for a miner. A single platform that allows one to receive many coins, could be even better. With FLDC being the flagship token of Merged Folding, all participants will receive this token from FoldingCoin Inc. regardless of the success or failure of other tokens on the platform. This allows miners to receive many coins that they can sit on or in some scenarios exchange for Bitcoin to help pay for the mining costs.

### 4.1.4 - Value For Mining costs

When mining with CPUs and GPUs hashing takes a drastic amount of energy and cooling in order to keep the chips from roasting. Folding@home and FLOPS don’t get nearly as hot. About half the electricity is necessary, since a different kind of computing cycle is used -- one that is not trying to brute-force a hash. In many cases, cooling systems may not even be required for folding.

### 4.1.5 - Value for helping small start-up coins

Devs of smaller startup coins spend most of their time trying to maintain a blockchain. Updating and securing a blockchain is a full time job. Many have neat ideas of having a coin used for something other than pumping and dumping. The success of a cryptocurrency depends on the dedication of the development team. The Merged Folding platform will empower the ability for token development teams to not have to maintain a blockchain anymore. Time can be focused now solely on the mission of creating a token with a use and to start working on features as well. They can now be more directly involved in their tokens community rather than QT wallet and source code.

- Other traditional altcoins having issues with hashing power or blockchain maintenance could make the move to Counterparty to harness the Folders' participation. These coins could hold their own burns, or FoldingCoin Inc. could help with a burn to exchange the original altcoin with the new Counterparty token.
- Many out there have great ideas for a coin, but don't want to deal with the wild west of altcoin mining. This gives them the ability to get their coin out there without having to worry about things like difficulty fluctuation and blockchain security updates. They will grow with Counterparty and their distribution will continue with folding power.

## 4.2.0 - Global Benefits

The amazing thing about non-profit distributed computing is no one is compensated for their work up to this point. This made sense back when distributed computing was first developed. It was a charitable thing to donate your computing cycles for science instead of giving money or volunteer hours. But when Bitcoin introduced a financial incentive to get more and more computational power for mining, competition, innovation, expansion, and commerce kicked in.

### 4.2.1 - Better use of energy for the world

There is no direct translation from one to another, but a common consensus is 1 hash equals 12,700 FLOPS when comparing the 2 side by side[25]. The FAH grid computing network has nearly 50 PetaFLOPS and is known as the world's most powerful computing network[26] outside of the Bitcoin mining network.

At the time before ASICs and FPGAs started hitting the market in December 2012, the Hash rate of the BTC network[27] was at 26 TeraHASH's in mostly GPU and CPU power. Based on a rough comparison 12.7 PetaFLOP = 1 TeraHASH the potential computational power that could be added to FAH is

**26 TeraHASH 12.7 PetaFLOPS = 330 PetaFLOPS.**

Imagine if that power was harnessed for molecular protein folding. Most of this power was redirected to altcoin mining after the SHA ASICs came out, since there was no profit motive for folding. FoldingCoin looks to bring a profit motive for people to fold proteins by distributing FLDC along with other Counterparty tokens.

### 4.2.2 - Venture Capitalists value

Venture capitalists could see this as an opportunity to invest in the creation of economic sized Anton Supercomputer, which is an ASIC molecular protein simulating machine that can fold more efficiently than standard computing hardware. This very thing happened to Bitcoin mining when it became exponentially profitable: venture capitalists invested in the creation of ASIC miners to compute SHA256 at a more efficient rate than standard computing hardware.

---

[25] Convert Hash to FLOPS http://en.wikipedia.org/wiki/Talk%3AFLOPS#Bitcoin_.22FLOPS.22_computation_on_bitcoinwatch

[26] Most powerful DCN http://en.wikipedia.org/wiki/List_of_distributed_computing_projects

[27] Bitcoin Network Hashrate https://blockchain.info/charts/hash-rate