Waste Not, Want Not: Your Computer Could Help Cure Cancer

A FoldingCoin, Inc. White Paper

Visit our website[1] or follow us on Twitter[2].

Authored By:

- Robert Ross - Administrator, Founder, Board
  rross@foldingcoin.net
- Miguel Molina – CTO, Board
  mmolina@foldingcoin.net
- Bill Beard Jr, - Executive Director
  bbeard@foldingcoin.net

[1] FoldingCoin Inc. Website: https://foldingcoin.net/

[2] FoldingCoin Inc. on Twitter: https://twitter.com/FoldingCoin

What If?

What if there was a cure for cancer in your lifetime? What if Alzheimer's was a thing of the past? What if redirecting wasted computing power could make these lofty dreams a reality? What if harnessing all that power was easy to do? What if you were part of the solution? What if you could personally benefit while contributing a little time to a cause so much bigger than yourself?

What is Protein Folding and Why Does It Matter?

Protein folding is the physical process by which a protein chain takes the shape necessary to perform a function in the human body, for example as part of cellular structure or as an antibody. It is central to healthy biological processes.

Cancer and Alzheimer's (among others) are well-known proteopathic[3] diseases, in which certain proteins become structurally abnormal, or misfolded. Scientists and medical researchers alike investigate why the proteins misfold and how medicines can be designed to correct the process. Gaining a deeper understanding of the protein folding process will get the medical community that much closer to curing these horrible diseases that have affected so many.

> *Gaining a deeper understanding of the protein folding process will get the medical community that much closer to curing these horrible diseases that have affected so many.*

Working the Problem: We Need More Power!

Due to the complexity of proteins' conformation or configuration space (the set of possible shapes a protein can take), as well as the statistically random, time-based nature of the modeling, it is exceptionally difficult to scale these simulations using general-purpose supercomputers. Such systems are intrinsically costly and typically shared among many research groups. So, how do researchers even begin to solve this massive computational problem? Enter 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 onto their own computers and leave the machines powered on even when not actively using them. The scientific investigators would use the leftover computing cycles to assist in solving their scientific problems.

An early example 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. Berkley's BOINC[5] is another example of a network with thousands of participants. However, there is one distributed computing project of particular interest in the fight against cancer.

[3] Proteopathy: https://en.wikipedia.org/wiki/Proteopathy

[4] Distributed.net: http://www.distributed.net/Main_Page

[5] Berkley's BOINC: http://boinc.berkeley.edu/

Folding@home

Stanford University started the Folding@home[6] project (FAH) in October 2000. The project runs computational algorithms to simulate the way protein molecules fold, and misfold, in the body. FAH is one of the world's fastest computing systems, with a speed[7] of approximately 135 petaFLOPS[8] as of January 2018. This power is faster than any 1 single supercomputer[9] in the entire world as of June 2018. This performance has allowed researchers to run computationally costly atomic-level simulations of protein folding thousands of times longer than formerly achieved. Since its launch, the Pande Lab has produced many scientific research papers[10] as a direct result of Folding@home that will help the medical community address critical protein misfolding problems.

Folding@home has allowed researchers to run computationally costly atomic-level simulations of protein folding thousands of times longer than formerly achieved.

Stanford launched its "I am One in a Million"[11] campaign to encourage volunteers to join the FAH network and to tell their stories about why they joined. The goal of the campaign is to reach one million volunteers to contribute their computing power to the project. As of June 2018, the campaign has achieved less than ten percent of that goal. At FoldingCoin, Inc., our primary objective is to help Stanford reach the one million mark and beyond. Before we can fully explain our approach, we must first lay the groundwork for the concept.

Digital Currency Mining: A Primer

Cryptocurrencies are digital systems (protocols) for exchanging value between participants on a decentralized computer network. Bitcoin (BTC)[12] is the most famous and widely adopted digital currency. Most cryptocurrencies use hard-to-solve cryptographic puzzles called "Proof of Work" to secure the operation of the network. Bitcoin uses the SHA256 hashing algorithm for Proof of Work. The process of verifying the cryptographic solutions is commonly referred to as "mining".

Finding the "solution" for a block (entry/record) is a vital operation to allow distributed consensus[13] and adds the block to the blockchain (database). Bitcoin introduced a "reward" system, where the miner who "solves" a block is awarded a small amount of the digital currency. This reward compensates the miner for contributing their hardware and electricity to securing the network.

The Shift to Mining Specialization

In the early days, a standard consumer or corporate PC could mine enough Bitcoin blocks using the CPU (central processing unit) and GPUs (graphics processing units) to turn a profit relative to the processing cost. Then, in 2013, the use of Application-Specific Integrated Circuit (ASIC)

[6] Folding@home Website: https://foldingathome.org/
[7] Folding@home live FLOPS: https://stats.foldingathome.org/os
[8] PetaFLOPS: https://en.wikipedia.org/wiki/FLOPS
[9] List of Super Computers June 2018: https://www.top500.org/lists/2018/06/
[10] Folding@home Research Papers: https://foldingathome.org/papers-results/
[11] Folding@home I am One in a Million Campaign: https://foldingathome.org/iamoneinamillion/
[12] Bitcoin: https://bitcoin.org/en/
[13] Distributed Consensus: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

mining hardware specializing in SHA256 began to dominate Bitcoin mining. This specialization, while beneficial due to reduced energy consumption, meant that it was no longer profitable to mine Bitcoin using general-purpose computers.

This shift led to the creation of hundreds of alternative cryptocurrencies, or “altcoins”, with their own blockchains trying to compete with Bitcoin. These altcoins tried to address the specialization by using the Scrypt hashing algorithm instead of SHA256. However, in early 2014, history repeated itself and Scrypt ASICs appeared, eliminating profitability for non-specialized mining. The shift left many former miners with lots of idle CPU and GPU time, freeing up valuable resources.

A Significant Source of Processing Power

Redirecting the unused computing power could more than double the processing power invested in computing protein folds.

While it is really not possible to measure the computational power of all of the CPU and GPU cycles no longer being used for mining, we can generate a rough estimate based on the following:

- At the end of 2012, the hash rate for the Bitcoin network was about 25 terahashes per second[14].
  - Since ASICs did not become common until 2013, we can assume that most of this processing was done using a standard PC CPU or GPU.

- 1 terahash : 12.7 petaFLOPS is a generally-accepted ratio[15].
  - Since hashing performs no floating point operations, there is no direct conversion from terahashes to petaFLOPS.
  - This ratio was derived based on side-by-side comparison.

Therefore, we arrive at the following estimate of the now unused computing power:

25 terahashes x 12.7 petaFLOPS/terahash = 318 petaFLOPS

Much of this power has been redirected towards other crypto chains that neither use scrypt, or SHA256 algorithms. Since the price hike of the crypto world exploded in 2017, it is safe to assume that this number is drastically higher than stated here as many looking to get into altcoin mining completely bought out inventory of GPUs[16] from all major outlets. It is safe to assume at this point that there are tens of thousands of GPUs being used for crypto mining. Redirecting the unused computing power of the former miners to the Folding@home network could alone more than quadrupling the processing power invested in computing protein folds. This understanding then leads us to the question: How do we get these miners (and others) to join the FAH network?

[14] Bitcoin Network Hash Rate: https://blockchain.info/charts/hash-rate?timespan=all
[15] Convert terahashes to petaFLOPS: http://en.wikipedia.org/wiki/Talk%3AFLOPS#Bitcoin_.22FLOPS.22_computation_on_bitcoinwatch
[16] CNET article: https://www.cnet.com/news/bitcoin-boom-pc-gaming-graphics-card/

Introducing an Incentive for Folding

Folding@home relies on the generosity of volunteers to donate their unused computing power to the project without any expectation of a return. When a donor joins the FAH project, he or she registers an account, installs a program, and FAH begins downloading "work units" to the computer. Work units are essentially "bite-sized" protein folding problems.

Who says we cannot offer both the noble and the tangible?

As a donor finishes a folding problem and submits the solution to FAH's server, he or she is awarded points and then assigned more work units. The more efficient one's computer completes work units, the more points one can earn. FAH's public statistics system[17] tracks all the work submitted, and points earned. However, these points offer no value beyond bragging rights.

One of the reasons that the Bitcoin network has grown so rapidly over the last several years is the potential for financial gain by earning Bitcoin in exchange for the processing power. While the notion of volunteering resources simply for the good of humanity is a noble one, our culture often looks for an immediate and more tangible return. Who says we cannot offer both the noble and the tangible? Indeed, we can.

FoldingCoin Inc. distributes cryptocurrency (tokens) to affiliated participants on the FAH network. The tokens are awarded proportionally, according to each participant's FAH points earned. These tokens can ultimately be exchanged for other forms of currency to offset the processing costs and even earn a profit. Next, we explain the token concept and how the tokens are distributed.

Tokens 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 innovative ways not envisioned by Satoshi Nakamoto and the early Bitcoin core developers.

FoldingCoin Inc. distributes cryptocurrency (tokens) to affiliated participants on the FAH network. The tokens are awarded proportionally, according to each participant's FAH points earned.

Counterparty[18] is a Bitcoin 2.0 system that allows users to create their own assets, often generically referred to as tokens, within the Bitcoin blockchain. It also offers a complete suite of financial tools. A project with a unique value proposition can use Counterparty's open source technology to create a digital currency token and then distribute those 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 Counterparty asset-related actions. The asset data is stored in bytes of available space that each Bitcoin transaction allows.

[17] FAH Team and Donor Stats: https://stats.foldingathome.org/donors
[18] Counterparty: http://counterparty.io/

Why Counterparty?

The Counterparty network offers a number of benefits that serve our mission:

- It leverages the security and stability of the Bitcoin platform, which in turn provides:
  - A large existing community with a vested interest
  - Management of the underlying blockchain functionality
  - Wallet support
  - Platform enhancements
- It prevents the introduction of more tokens into the market using a “locked asset”.
- It requires no direct mining of assets.
  - Therefore, token creation and transfer can be verified on third-party sites such as xchain.io and still also be verified by Bitcoin miners.

However, we must also address some significant concerns that come along with this choice.

Security and Accountability

Using Counterparty tokens instead of those created when hashing a decentralized blockchain means it is incumbent on the creator to have high standards for security and accountability.

We take the security of the undistributed tokens very seriously. Token distribution requires the private keys held by two of the board members, as well as the third key held by a trusted third party. As an Indiana non-profit corporation with 501(c)3 charity status, FoldingCoin Inc. must abide by all applicable US federal and state laws. The Folding@home project is the sole beneficiary of all assets in the event of dissolution.

What is FoldingCoin?

FoldingCoin (FLDC) is a Counterparty token created as a “cause coin” with a “Proof of Fold” concept to verify contributed computational power. Since Counterparty tokens share the Bitcoin blockchain, the security and hashing rate are already covered, eliminating the need for a “Proof of Work” algorithm used for traditional altcoins.

Only one billion FLDC tokens were created, and the asset was then locked, making it impossible to issue more. Ten percent (100 million) of the tokens have been designated as a means of compensation for development work contributed to the project. We track the development payouts on the FoldingCoin website[19].

FoldingCoin (FLDC) is a Counterparty token created as a “cause coin” with a “Proof of Fold” concept to verify contributed computational power.

FoldingCoin Distribution

The “Proof of Fold” can be manually computed since the FAH statistics are posted publicly online and readily available. The statistics are provided in the form of a text file[20] listing every volunteer (or “folder”) lending computing power and contains the total points earned as of the last update. FAH updates the statistics once an hour.

[19] FoldingCoin Development Payouts: https://foldingcoin.net/index.php/about/financials
[20] FAH Statistics File: http://fah-web.stanford.edu/daily_user_summary.txt.bz2

Once a day, our Download Calculator downloads the FAH daily user summary and searches to find those folders who have set up their folding software using the required address format. The code then calculates the new points earned that day. On the first Saturday of the month, the team runs a report from the previous month that adds up the daily FAH points earned. Finally, we calculate the FLDC tokens due each valid folder based on the current FLDC amount per FAH point. The reports and distribution[21] information are available on our website.

FoldingCoin has partnered with Tokenly to offer the Merged Folding Distributor[22] an all-in-one solution that allows us to create a distribution address used to send out the FLDC earned. Once the distribution is executed, a Counterparty-enabled address will batch all the required FLDC payments and send them out to the network. This method avoids having to send payments one-by-one to individual participants, and the platform also supports distributing other Counterparty tokens.

The manual process of submitting the transaction to Tokenly gives our team the opportunity to review the information for accuracy and correct any mistakes. As a 501(c)3, we believe the public nature of our organization will maintain the necessary team engagement required to ensure the continued distribution of FLDC tokens in exchange for participants valuable unused computing power.

There are no service fees for FLDC distributions, as they are funded by the organizations own financial holdings.

What about the ASICs?

You might be thinking: Why should I get involved if someone is just going to build a specialized machine or environment to do all of the folding and earn all of the FLDC tokens? That is a great question, and the answer is simple: money. In order for an ASIC to contribute folding power to earn FLDC, one would either have to get a hold of the Anton supercomputer[23], which is an ASIC specifically designed for protein folding, or perhaps an Amazon EC20 instance. Both are so expensive that the possibility of earning a profit would be out the window. However, if the unimaginable did happen and a consumer grade ASIC was created for protein folding simulations, it would simply mean much more computing power would be devoted to our ultimate goal of finding a cure. Like Bitcoin, in which ASIC miners have helped drive security up for the blockchain, ASIC Folder's would help drive up computing speed which is also a good thing for the research.

[21] FLDC Distributions: https://foldingcoin.net/index.php/resources/distributions
[22] Merged Folding Distributor: https://foldingcoin.net/index.php/merged-folding/what-is-merged-folding
[23] Anton supercomputer: https://www.psc.edu/resources/computing/anton

Stay Tuned

At FoldingCoin Inc., we are just getting warmed up. We are diligently working to provide more ways to engage our community of folders and provide tools to make earning FoldingCoin easier and more fun. These include a loyalty program and a statistics page for tracking FoldingCoin earnings.

Our mission is to redirect the massive distributed computing power used in alternative digital currency blockchains to be better used for medical and scientific projects working to find cures and solve other world problems.

In the meantime, join us on Discord[24] (see our FAQs page[25] for the roles, rules and bot commands) to engage with the developers and other members of the community. We are looking forward to seeing you there!

About Us

FoldingCoin Inc. is an Indiana nonprofit corporation[26] with a 501(c)3 IRS status, formed under the Indiana Nonprofit Corporation Act of 1991. Our mission is to redirect the massive distributed computing power used in alternative digital currency blockchains to be better used for medical and scientific projects working to find cures and solve other world problems.

[24] Discord Community: https://discordapp.com/invite/xhth8cR
[25] FoldingCoin FAQs Page: https://foldingcoin.net/index.php/faqs
[26] Indiana Nonprofit: https://bsd.sos.in.gov/publicbusinesssearch