Paul Chou

Foundation Coin
A Cryptocurrency Architecture Designed for the Solar System

Introduction

This white paper describes a new proposed cryptocurrency ("Foundation Coin") designed for the unique requirements of solar system distances. In particular, it retains most elements of the original Bitcoin architecture with a fundamental difference in the structure of the blockchain itself.

The challenge addressed by Foundation Coin is to ensure crypto's integrity in maintaining a distributed, consistent ledger among all participants when communication across large distances no longer resemble the relatively low communication lag enjoyed on Earth.

The architecture of the original Bitcoin protocol by Satoshi Nakamoto has a design optimized for earth-based ledger synchronization. In particular, the 10 minute average block timing gives all participants (miners) the chance to find the next block in the chain. But crucially, 10 minutes also gives sufficient time through modern internet fiber connections to allow all participants quick synchronization for the latest valid block.

These assumptions break down at the solar system scale; in particular, Mars. If one of the key requirements of a robust cryptocurrency is synchronization of the ledger to guarantee fairness between all participants, then the solar system scale breaks a lot of the original Bitcoin constructs.

Take the example of trying to maintain a single, consistent ledger of all transactions between Earth and Mars. Due to the immense distances, and critically, the variation in distance between the planets as the orbits change, the distribution of the most recent ledger can be significantly delayed simply due to the speed of light.

Over the course of approximately 2.2 years, due to the variation of Earth / Mars co-orbits, the time to communicate between the planets changes dramatically. At the closest point, the speed of light takes 3 minutes to go from Earth to Mars, and vice versa. Factoring in that we want to compensate for round-trip time (for Earth to send the latest ledger to Mars, and have the Martians, upon receipt of the latest ledger, send their new transactions to Earth to be entered into the transaction pool), we have to double that number. This requires a 6 minute delay (a halt on adding new transactions to the next block, until the communication can be synced).
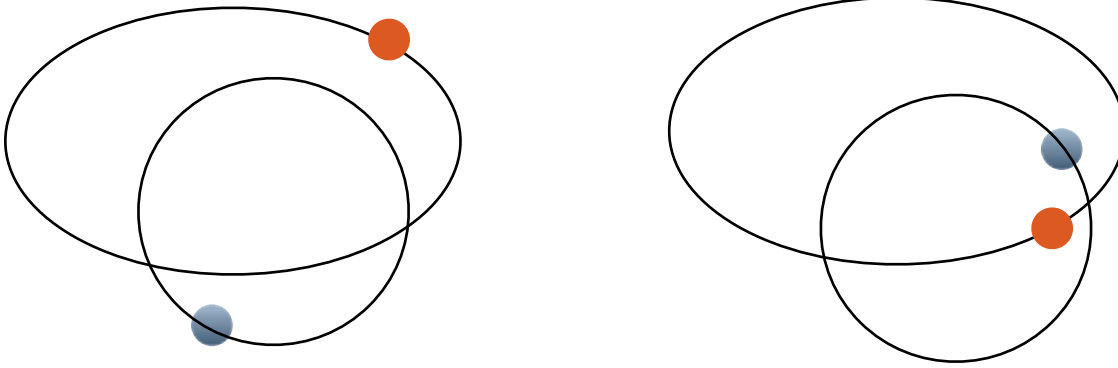
Figure 1. A rough depiction of how orbital variations can cause large variations in straight line distance between the Earth and Mars. Communication times, even at the speed of light, will vary dramatically.

At the farthest distance in the Earth / Mars orbits, the speed of light takes 22 minutes, one way. Doubling that again, it implies a 44 minute wait time to ensure both ledgers are received and synced before adding new transactions to the overall blockchain.

A Revised Blockchain Architecture—Introducing "Transit Blocks"

One of the fundamental innovations of Foundation Coin is a revised blockchain architecture to address the variation in sync delays. Whereas Bitcoin proper uses the traditional chained transaction blocks:
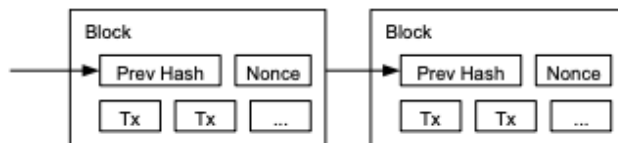
Foundation Coin will alter the architecture to alternate transaction blocks with "transit blocks." These represent the time delay for information to transit at the speed of the light, round trip, between Earth and Mars at the current orbital context:
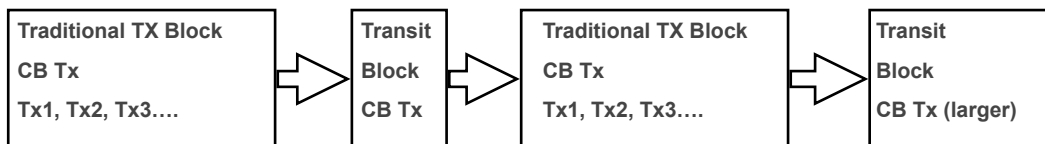
The interspersing of transit blocks between normal transaction recording blocks enforces a time buffer. Foundation Coin calculates the time that the current transaction block is being mined and can reference the time/date/year of that block to understand how far (or close) Mars is to Earth at that very moment. It then calculates a Transit Block with a target time delay to allow a round trip propagation. As the above diagram is attempting to illustrate, the length of time for the transit block is varied, depending on the current orbital situation between the two planets.

The transit block is different from traditional Tx blocks in that the time for it to be mined is determined by the orbital situation, and it does not allow for the embedding of any actual transactions. A single transit block coinbase transaction is allowed, so that miners are incentivized to continue investing proof of work while "waiting", therefore continuing to strengthen the overall chain as PoW is designed to do.

The transit block allows miners to continue receiving traditional block rewards while allowing sufficient time for the last transaction block to be broadcast to Mars. When it's received there, the Martians have sufficient time to see the latest ledger and broadcast their own transactions back to earth to join the traditional transaction pool. After that, the whole sequence starts again. The round trip calculation / delay is what allows this architecture to sync correctly.

Conclusion

Foundation Coin is a cryptocurrency design for a very specific purpose—to be an efficient, fair, gross settlement system for solar system scale value movement. It is not designed to optimize for transactions per second (credit cards), or as a net settlement system (ACH). The closest analogy would be to a fed wire system for large, irreversible movements of money designed with a crypto architecture that incorporates adjustments for solar system scale considerations.

Given recent advances by private space companies and increasing peer super power competition to colonize the Moon, Mars and perhaps other celestial bodies, Foundation Coin is envisioned to play a long-term financial part in these advancements. With an architecture such as this in place, future colonists on Mars, upon discovering an opportunity to build a mine or other critical infrastructure as they explore the planet, can request and receive near immediate investment from Earth and do so in a way that is apolitical and free from traditional US banking constraints.

Finally, why the name "Foundation" coin? It is a nod to the classic Isaac Asimov trilogy—if Earth is our Trantor, then Mars is our Terminus.

Foundation Coin is designed to be the modern financial bridge between those two economies.