Building "Mars Coin" on Holochain

Perry Kundert

2021-04-11 06:55:00

We propose that it's possible to build "Mars Coin" on Holochain (PDF/Text).

Now that lunar and interplanetary expansion appears to be a realistic goal, how will cryptocurrency transactions be affected by the communications time between earth, the moon and other planets in our solar system? It takes between 5 and 20 minutes for one-way communications between Mars and Earth (depending on their orbital positions), and 2.4 to 2.7 seconds between Earth and Moon.

Cryptocurrencies based on global consensus algorithms (eg. Bitcoin, Ethereum, Dogecoin, Hashgraph, ...) require **at least** a single one-way communication (simultaneously, in both directions) to transmit the facts required to achieve a consensus "total order" of transactions.

Holochain hApp DNA code (the Rust code, compiled to WASM, that defines the Holochain application, or "hApp") could use such global consensus algorithms when required, but direct agreement between a small set of agents (often nearby each-other) is usually adequate. For example, agreeing to transfer amounts between agents' ledgers is quite simple, and certainly doesn't require the global consensus of all agents! Detection of fraudulent transfers is also simple, and automatic – any transfer so agreed between agents that *doesn't* comply with the rules of the particular cryptocurrency's "DNA" code are immediately marked as fraudulent, and all agents involved are self-incriminated by their cryptographic signatures on the transaction.

Therefore, a Holochain "Mars Coin" could sustain billions of aggregate transactions per second across multiple planets in our solar system. Transactions would be "finalized" at a rate on the order of a single round-trip between the *specific* agents involved (virtually instantly, if the agents are co-resident on the same planet's network), and confirmation of absence of fraud would be automatic and verifiable after simply *waiting* for single one-way communications latency to elapse.

Contents

1 Global Consensus Between Planets

The Marscoin project proposes, correctly, that existing global consensus based cryptocurrency systems cannot work efficiently in high-latency communications environments. Even if the block-to-block consensus time was stretched out to 40 minutes (to encompass the longest round-trip time between Earth and Mars), the proof-of-work miners on Earth and Mars would be wasting resources mining on top of the "wrong" chain during the communications delay – they would each waste around 1/2 of their "mining" resources, on average.

1.1 Consensus Under High Latency

If a cryptocurrency demands global consensus to establish a "total order" of all transactions, the communication latencies required to establish this consensus apply to *every* transaction – even transactions between agents very close to each-other!

For blockchains with "statistical" finality like Bitcoin, Ethereum, Dogecoin etc., this would entail up to hours of delay between transaction initiation and likely finality. Systems with "cryptographic" finality like Hashgraph require two full round-trip latencies to reach finality, but this still limits aggregate transaction rate, since each agent typically must await finality of their current transaction before executing the next; or, if pipe-lining of transactions **is** supported, a counterparty must wait for finality of their particular transaction before exchanging the good or service – which requires that all nodes receive gossip of later events before prior events can be correctly placed in a consensus "total order".

This means that events between agents co-located together on Earth, or the Moon or Mars must await the reception of events from these other distant locales before the local events can be finalized.

Thus, the absolute lower bound on finality must be **at least** one full body-to-body latency period; eg. 5-20 minutes for a global consensus system including agents on Earth, Moon and Mars.

1.2 Energy Usage Implications

The energy required to achieve global consensus is a real and significant cost, especially for PoW systems like Bitcoin and (presently) Ethereum. As system-wide latencies increase, more and more of this energy is wasted due to nodes "working" on the wrong fork.

Even the most energy-efficient implementations of global consensus such as Hashgraph aBFT (orders of magnitude better than Bitcoin) still expend this energy unnecessarily!

Holochain avoids this energy expenditure completely, by only achieving direct consensus between the set of agents involved in a transaction, and by spreading the global transaction DNA validation load onto the minimum subset of randomly selected agents required to achieve a desired level of correctness certainty, appropriate to the problem being solved. This might be very high for a Holochain-based cryptocurrency such as "Mars Coin", and much lower for a game.

As a result, huge, solar system spanning Holochain networks can be created that perform billions of aggregate transactions per second very efficiently, and waste comparatively little energy.

2 Holochain Agreement

The agent-centric Holochain system provides a foundation for scalable shared systems such as cryptocurrencies that span our solar system.

Instead of a single, shared data-centric consensus view, giving every agent an identical "total order" view of all events (from which a single global "state" can be deduced by all participants), Holochain implements a consensus agreement on rules agreed upon for all interactions between agents.

Every participant agent agrees that they wish to join in a distributed, shared application with certain rules, and every agent node ensures that every DHT entry they host (a copy of a commit by some agent in the shared application) follows these rules. A *single* non-fraudulent DHT agent is all

that is required to detect a fraudulent transaction. The DHT entries generated during the course of each transaction are automatically propagated to many DHT nodes situated in all planetary bodies hosting the multi-planetary DHT, so any fraud is immediately detected, in every locale, as soon as it arrives there.

These rules *could* include, if desired, an implementation of an aBFT global consensus total order based on median signed validation timestamp (like Hashgraph). This might be necessary for certain applications, such the core order-book matching component of a decentralized trading platform.

More often, much simpler and less complex and expensive forms of agreement are adequate. A simple cryptocurrency can be implemented by multiple agents countersigning the identical record of transfer of amounts between their ledgers to transfer funds in a mutual credit cryptocurrency system, with validation that no sum of balance + credit is allowed to go below zero (with, of course, at least one node allowed by the hApp DNA rules to issue credit).

Any agent that crafts and signs a commit that *violates* the agreed upon DNA rules will be detected and "Warranted" by the *first* non-fraudulent DHT node that hosts such a commit. Every other node that considers dealing with the agent can easily confirm the claimed fraudulent behaviour, and reject the fraudulent node.

The entire "tree" of transactions is proven valid by induction; if no commit is validated until the *prior* commit is validated (is also seen in the local DHT), then *every* commit back to the "epoch" for each agent is also known to be valid – thus, *every* cryptocurrency ledger transfer leading to a current ledger balance is known to be valid. As the pool of DHT agents validating is constantly changing and the DHT validators are unpredictable to the transaction participants, no invalid DHT entry can remain hidden (eg. hosted only by complicit agents), no matter how powerful the fraudulent adversary is in the network. There is no "50% + 1" attack; a *single* non-fraudulent node *anywhere* in the network is sufficient to cryptographically detect, prove and destroy an attack – even if they hold 99.999% of the network "power".

2.1 Agreement Under High Latency

Holochain requires a two-way communication between each party to reach agreement on a particular transaction, because *global* consensus is not required for most interactions (and certainly not for a "total order" of *all* transactions).

Reaching this agreement between two agents typically requires a single round trip; one trip to provide the first agent's validation state and the

proposed transaction to the counterparty, and then one trip back to provide the first agent with the second agent's approval, and all of its validation state back to the first agent.

Therefore, agents nearby each-other can proceed as fast as their communications channel, computation and storage allows; potentially, executing and completing thousands or even millions of finalized transactions per second (if so required and optimized for). This transaction throughput scales linearly with the number of agents; in aggregate, billions of system-wide, finalized transactions per second are possible – easily handling any foreseeable transaction load required by an interplanetary monetary system.

2.2 Assurance of Validity

If DHT validators can immediately detect attempts at fraud, an attacker could perform some valid transactions (eg. accumulate a valid, positive cryptocurrency ledger balance), and then attempt to *use* the communication latency between planets to attempt to perform one or more "double spend" transactions.

By duplicating the agent's private source-chain simultaneously in 2 or more places separated by long communication latency, each copy of the agent and its source-chain could attempt to simultaneously "spend" the same balance! The same (currently valid) agent source-chain would be "forked" in each separate communication context. This fork is trivially and automatically detected as soon as the commit is "gossiped" to DHT agents across the latency divide.

2.2.1 Detecting Fraud

If desired (ie. for high-valued transactions), a recipient agent might choose to simply *wait* for the duration of a single one-way communications latency period. By waiting before delivering the agreed upon product or service, the agent ensures that the counterparty hasn't attempted to "fork" their personal source-chain on another planet. If the counterparty did attempt fraud, the evidence (in the form of DHT records indicating a "fork" of the agent's source-chain) would appear locally after a single one-way latency period, as they are automatically published to many agents in every other locale.

Attempting a double-spend would thus immediately be detected and produce a "Warrant" implicating the agent(s), and *destroy* the fraudulent

agents' ability to ever transact again – the instant the DHT entries containing the "fork" propagate to a single DHT node on the other planet.

3 Results and Future Developments

Several prototype implementations of Mutual Credit cryptocurrencies have been developed and tested. The future "Holo Fuel" implementation underpinning the Holo system will be deployed soon, with other specialized community currencies and general purpose multi-currency Mutual Credit ledgers currently in development.

A demonstration of a prototype "Mars Coin" is under development, to demonstrate these claims and benefits of the agent-centric Holochain model of distributed application architecture.

By the time we have humans in transit to the Moon and Mars, they should be able to carry with them a multi-planetary cryptocurrency implementation suitable for use between all the planets where humans thrive!