

An aerial view of a futuristic Martian colony. The landscape is reddish-brown. The colony features various structures, including large domes, smaller buildings, and a network of roads or paths. A prominent yellow and red diagonal graphic is overlaid on the left side of the image. The title text is centered in the upper right quadrant.

Planetary 'Hash-War' Protection as an Example of Decentralized Licensing Systems

Martian Republic Series

Martian Republic

A quick review

Motivation and Purpose





What is The Martian Republic?

The Martian Republic is an online decentralized p2p governance system allowing Martian settlers to engage in all civic tasks necessary for a direct democratic state.

This new form of “Republic as a Service”, in which each citizen is an active representative of the state, achieves a new level of transparency deriving a cryptographically secured direct and immediate consent of the governed.





Understanding the problems

- 01 We seek to create a direct democratic congress of citizens - disintermediating a vulnerable “man-in-the-middle” attack of lobbies and politicians “buying votes”.
- 02 We try to avoid unnecessary complexity in favor of ultra-transparent and self-evident cryptographically secured and easily auditable votes.
- 03 We avoid scaling issues by building our infrastructure on a server/client architecture and open source code. Individual nodes can be taken down, but the rule-set and data lives on as long as one peer survives.





What the Martian Republic seeks to accomplish...

We achieve a highly dynamic self-correctable system of governance in which each citizen directly impacts the very code and rule-set on which the community operates.

- Tamper-proof decision making
- Minimizing special interests
- Effective and transparent
- Minimizing bureaucracy
- Governance automation
- Immutable audit trail
- Privacy conscious



Decentralization at the core...

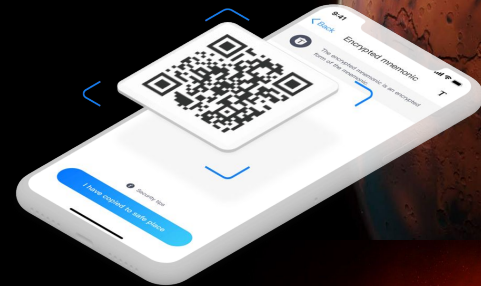
The Martian Republic is built upon four core technologies:*

Distributed / External

- *Marscoin - PoW blockchain as immutable trustless public ledger*
- *IPFS - Decentralized data storage system*

Server-Client / Internal

- *Non custodial online wallet*
- *Coinshuffle protocol*



IPFS





Martian Republic

Hashwar Protection

Solving planetary licensing issues in a decentralized disintermediated democratic system



The premise

The Lightspeed / Distance
Necessitates separate
blockchains

Any realtime protocol fails to allow Martians to participate in Bitcoin mining and delays the confirmation time between blocks (they would most likely get a cached version of the blockchain every so often - think 20 minute increments). A space suit rental on Mars does not want to wait for several cached downloads of a Bitcoin blockchain even if it's incremental - to make sure that it's financial transaction got settled. Martians will use their own public blockchain to transact, vote and audit. Marscoin.

A problem arises

The vulnerable Martian blockchain could get out-run by Earth based miners

If Martians run their own blockchain they will run into the issue that Earth miners with their superior hardware might decide to attack the martian blockchain and roll it back a few blocks by downloading a larger chain that was mined on Earth and "front-ran" the martian chain, thus allowing evil actors to double spend or otherwise influence the Martian sovereign financial or worse yet - political / administrative network.

An easy fix, a bad solution

Creating a central authority to regulate a decentralized process?

However, if the Martians decided to control the individual martian miners and only allow digital signatures from local miners they would typically need a central authority that issues such "licenses" and modifies the marscoin network to reject any other blocks. But we do not want any central authority - which defeats the entire purpose of running a decentralized blockchain. So what's the solution?

A better solution

The Martian Republic decentralized governance system is itself used to issue licensing!

We demonstrated in 2022 a voting system built into the Marscoin blockchain - a public on-chain voting system using coinshuffle protocol and public voter registries to allow for transparent, auditable, private, cryptographically secure voting to take place. We here propose to use that "Martian Republic" governance system to publicly allow Martians to register their mining equipment with the public governance system and get the up-vote of enough Martians to become contributors of the mining entities that support the financial system. These "licenses" are just one example how the "hive mind" of the Martian Republic can add and revoke licenses granted to individuals.

How exactly?

The Miner example

1. In this particular case these licenses are probably the most fundamental as they keep the entire system functioning and protected from Earth.
2. The way it works is that an endorsed Martian (upvoted by a sufficient number of fellow Martians) publishes his mining software's public key.
3. Whenever this miner finds a new block, he will sign the new block hash with his public key that's visible to all. If the digital signature is valid (any node in the network can check and test signature+public key) it is a block that the network will adopt.
4. If the miner does NOT have a valid digital signature in his block, the block gets rejected.

What are the benefits of this approach?

- Works for any licensing regiment
- Protects the network in a decentralized and dynamic fashion
- No central arbiter needed
- Disagreeing factions can fork and split off yet retain absolute transparency

In general all government activities are intended to occur online and make use of private-public key secured digital signatures.

Martian Republic

Final Thoughts

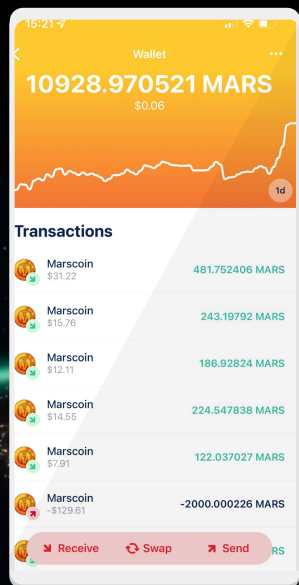
The Future of the Martian Republic



Decentralized P2P governance -
Creating a hive mind on a planetary level

...while safeguarding individual rights

The Martian Republic
ephemeral yet
immutable.



Open to anyone - belonging to no one


“The right of voting ... is the primary right by which other rights are protected. To take away this right is to reduce a man to slavery, for slavery consists in being subject to the will of another, and he that has not a vote ... is in this case.” - *Thomas Paine*

“Most likely the form of government on Mars would be a direct democracy, not representative,” said Musk. “So it would be people voting directly on issues. And I think that’s probably better, because the potential for corruption is substantially diminished in a direct versus a representative democracy.” - *Elon Musk*

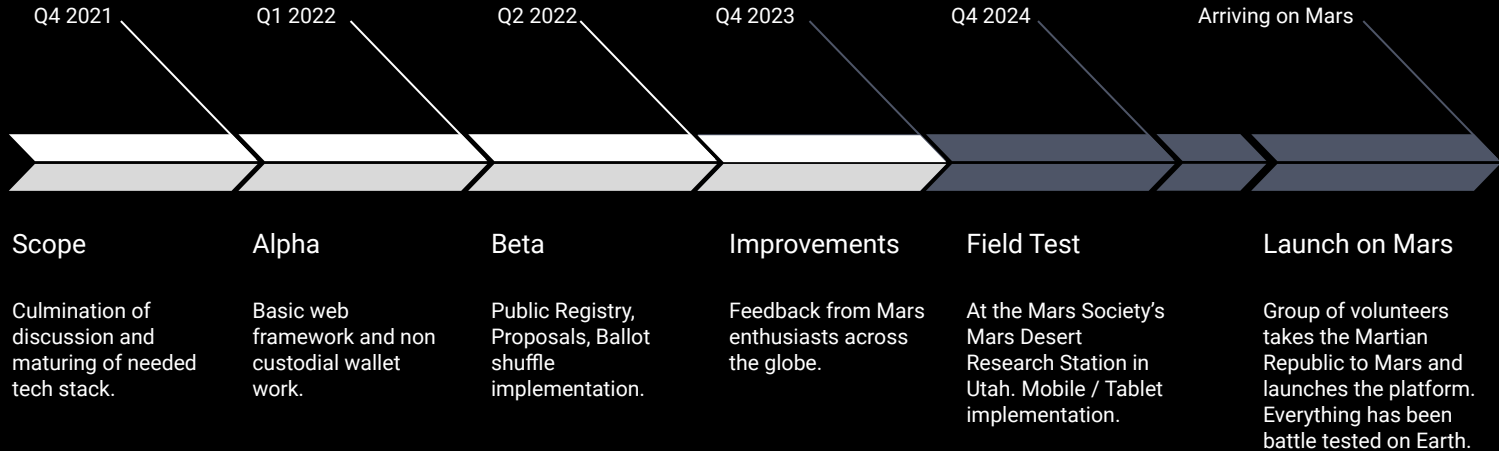




Caveats

- 01 The Martian Republic depends on a well distributed mesh network of IPFS nodes to minimize data loss. A large node network is desirable.
 - 02 The Marscoin blockchain security against 51% attacks improves with a mining algorithm that fosters wide adoption and minimizes mining centralization.
 - 03 The ballot shuffle procedure requires participants to remain online until their ballot has been received. More client implementations (mobile, pine phone, etc.) and improved robustness / scalability tests are required.
- 

Project timeline



Mission objective

A bootable self-contained distribution consisting of...

- Marscoin source code
- Marscoin blockchain
- IPFS source code
- Martian Republic source code

... to jump-start a Martian Civilization





Thank you!

Heartfelt thanks to the entire
#OccupyMars universe of wonderful
human beings around the world.
Special thanks to The Mars Society,
SpaceX and everyone working
tirelessly getting us closer to the stars
and out of the cradle...

Planetary 'Hash-War' Protection as an Example of Decentralized Licensing Systems

Lennart Lopin

Abstract

The remote nature of Mars necessitates a financial system tailored to its specific challenges. Traditional blockchain protocols face latency issues arising from light-speed communication constraints, rendering real-time transactions on Mars less than ideal. Moreover, the potential exploitation from Earth-based miners, equipped with advanced hardware, introduces risks such as double spends.

Building on the foundation of the Martian Republic—a blockchain-based "Republic As Software" system that achieves transparency and direct participation—this paper emphasizes the evolution of its public voting system, which leverages the coinshuffle protocol. While the voting system itself is a testament to decentralized governance, our primary focus is on the innovative approach to its application. We propose using this existing voting system for a community-based licensing process. By allowing Martians to register their mining software's public key, and subsequently seeking community endorsement via votes, miners can earn the community's trust and validation. Once endorsed, miners can then sign blocks with their digital keys. Only blocks carrying these community-approved signatures are integrated into the blockchain, while those without are dismissed.

This novel approach to licensing accentuates the collective power and decision-making capability of the Martian community, ensuring that it remains decentralized and free from any central authority's undue influence. By intertwining the coinshuffle voting platform with a digital signature-based validation system, the Martian Republic not only fortifies its network against hash attacks but also enhances security and auditability across various community actions and processes. In an era of burgeoning interplanetary settlements, our approach underscores the Martian Republic's dedication to ensuring that its blockchain governance remains transparent, auditable, and truly representative of its community's collective will.

1 Premise

We have the following issues: a planet at substantial distance from Earth (think Mars) necessitates its own blockchain due to light speed limitations in data transfer. Any real-time protocol fails to allow Martians to participate in Bitcoin mining and delays the confirmation time between blocks (they would most likely get a cached version of the blockchain every so often - think 20 minute increments). A space suit rental shop on Mars does not want to wait for several cached downloads of a Bitcoin blockchain even if it's incremental - to make sure that it's financial transaction got settled.

However, if Martians run their own blockchain which brings more benefits than just planetary sovereign control over their financial independence (think voting) they will run into the issue that Earth miners with their superior hardware might decide to attack the martian blockchain and roll it back a few blocks by downloading a larger chain that was mined on earth and "front-ran"



Towards a Multi-Planetary Humanity

“The Earth is the cradle of humanity, but mankind cannot stay in the cradle forever.”

Konstantin Tsiolkovsky

“Why should humans go to Mars? There are really three reasons: for the science, for the challenge, and for the future.”

Robert Zubrin

