The Martian Republic - A governance system for Mars

Sebastian Fabara, Lennart Lopin, Philipp Puaschunder, Matt Wise

Abstract

The Martian Republic is a suite of online tools built around an online non-custodial wallet, allowing the early Martian settlement to offer all necessary civic tasks in building a direct participatory democratic society. This new form of blockchain-based "Republic As Software" achieves a high level of transparency in direct and immediate consent of and by the governed. Each participant is an active member utilizing censor-resistant public forums and casting cryptographically secured and end-to-end auditable votes. The very codebase on which this Republic runs becomes its Constitution and remains a reflection of the will of the people. Each individual directly interacts with society leveraging the advantages of trust-less ledger technology for notarized on-chain actions. The client-server open-source second-layer caching solution provides a scalable architecture. To this end, the project ties together a secure proof-of-work blockchain (*Marscoin*) and a modern distributed data storage system (Interplanetary File System or *IPFS*). We propose this coordinated tool-set approach, that links a wallet, a dynamic public voter registry, a public forum, and a coinshuffle-based secure ballot issuance, to derive a unified public consensus. We present this combination of an initial set of tools, the Martian Republic, as a unique governance platform to which other organizational features can be added dynamically over time and which, being software itself, is allowed to consensually develop as society evolves.

1 Introduction

> *Congress*...the supreme legislative body of a nation and especially of a republic[4]

> *Martian Congress*: An on-chain, transparent, end-to-end auditable governance system utilizing a non-custodial wallet, public voter registry and a coinshuffle-based encrypted ballot distribution system to ensure fair voting on public proposals by secret ballot.

A purely on-chain, cryptographically secure voting process would allow each citizen to participate directly in the formation of a Republic in which matters of the public (*"res publica"*) are decided by a congress consisting of the very public itself, without the need for intermediaries.[1] [2]

[1] Wikipedia[1]: "...relevant to the history of direct democracy is the history of Ancient Rome, specifically during the Roman Republic, traditionally founded around 509 BC. Rome displayed many aspects of democracy, both direct and indirect, from the era of Roman monarchy all the way to the collapse of the Roman Empire. While the Roman senate was the main body with historical longevity [...] it did not embody a purely democratic approach, being made up – during the late republic – of former elected officials, providing advice rather than creating law. The democratic aspect of the constitution resided in the Roman popular assemblies, where the people organised into centuriae or into tribes – depending on the assembly – and cast votes on various matters, including elections and laws, proposed before them by their elected magistrates. Some classicists have argued that the Roman republic deserves the label of "democracy", with universal suffrage for adult male citizens, popular sovereignty, and transparent deliberation of public affairs. Many historians mark the end of the Republic with the lex Titia, passed on 27 November 43 BC, which eliminated many oversight provisions."

[2] Kurland[2]: "The slogan 'No taxation without representation' is a response to offended notions of rights, equity,

Since the invention of the internet many trust- and authority based systems have been made superfluous as their information arbitrage advantage ceased to exist. Satoshi Nakamoto's invention of a distributed trustless ledger system, Bitcoin, took this innovation into the realm of economics, politics and law.[3] The Martian Republic is an implementation on top of these innovative technologies and a chance for citizens to "represent themselves"[4], to express the sovereign will directly and tamper-proof through open public discourse, procedure and vote.

Utilizing a blockchain to timestamp proposals and identify the members of the public is part of the solution, but benefits are lost if reliance on unmanageable databases or staked tokens make voting via smart contracts vulnerable to Sybil attacks.[5] The Martian Republic's Congress module attempts to overcome such limitations and seeks a transparent and simple as possible solution which allows all participants to **easily audit and verify the validity of their vote**. By utilizing an open source model in which the code itself becomes the Constitution, we opt for a server/client architecture in which the initial participants curate via transparent rules a public voter registry. Any member of this assembly of citizens can then initiate proposals, submit code changes ('amendments') or suggest alternative configuration settings ('statutes', 'regulations') etc.

These proposals are stored in a decentralized fashion using IPFS and are thus available in an – ideally – planet-wide operating public mesh network. Additionally, each proposal is hashed and notarized on the blockchain for added censor resistance. A citizen's ability to suggest code changes to the codebase of the Martian Republic itself is the most direct expression of public intent. Such a 'pull-request' once voted into law becomes part of the very mathematical rules that dictate the fabric of the governing system. Software replaces law-making as far as the realm of software extends and can replace ambiguous human language with the mathematical precision of programming languages. As the server restarts in regular intervals, the system is capable of inheriting voted-upon changes. As the code is open source, any dissenting faction can - in theory - suggest changes at any time or break off and start its own entirely new offspring elsewhere motivating the assembly to carefully discuss and include all viewpoints.

Each proposal launches "ballot-shuffle" server sessions in which participants request private ballots for a particular vote. The *ballot-shuffle* is built on the "coin-shuffle protocol"[6] which obfuscates transactions of many participants on the blockchain and prevents third parties from tracing votes back to individual citizens. The ballot-shuffle makes it easy to authenticate participants (one-vote-per-citizen, all shuffle participants appear in the voter registry, with one single vote irrespective of individual net worth). At the same time it ensures private and fair votes without any participant's (nor the server's) knowledge of an individual's vote. Various proposal run times and percentages

and good sense: rights, because no part of any man's property can be taken without his or his representative's consent, or if taken without consent, only at the price of impoverishing the people and robbing men of an essential support of liberty (see ch. 17, no. 5); equity, because those who bear a burden ought to have a voice; good sense, because governors needlessly deprive themselves of a valuable source of information by excluding those who best know their situation (nos. 4, 8). Given this line of reasoning, why ought there to be representation at all? **The obvious answer is that the people in a numerous and extensive commonwealth cannot conveniently assemble as a whole**. To stand for the people, a representative body should then be a representation of the people or (more strictly) of the citizenry (no. 12; see also ch. 17, no. 9).

[3] Satoshi Nakamoto's seminal " Peer-to-Peer Electronic Cash System" [3].

[4] "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." [5]

[5] For attacks against identity systems underlying anonymous smart contract systems see [6].

[6] "CoinShuffle: Practical Decentral- ized Coin Mixing for Bitcoin" [7].

of citizens required to participate before a bill passes, are variables, that the public itself agrees upon. The Republic thus becomes a living software structure in which all members of the public are similarly citizen, assembly of congress, and representatives of their Republic - fulfilling an ideal that has been elusive since antiquity due to the missing link of cryptography and modern networking technology.

2 Overview – The Martian Congressional Republic

The Martian Republic is built around a modern non-custodial browser wallet and the following suite of tools that interconnect (see `martianrepublic.org` for a live implementation).

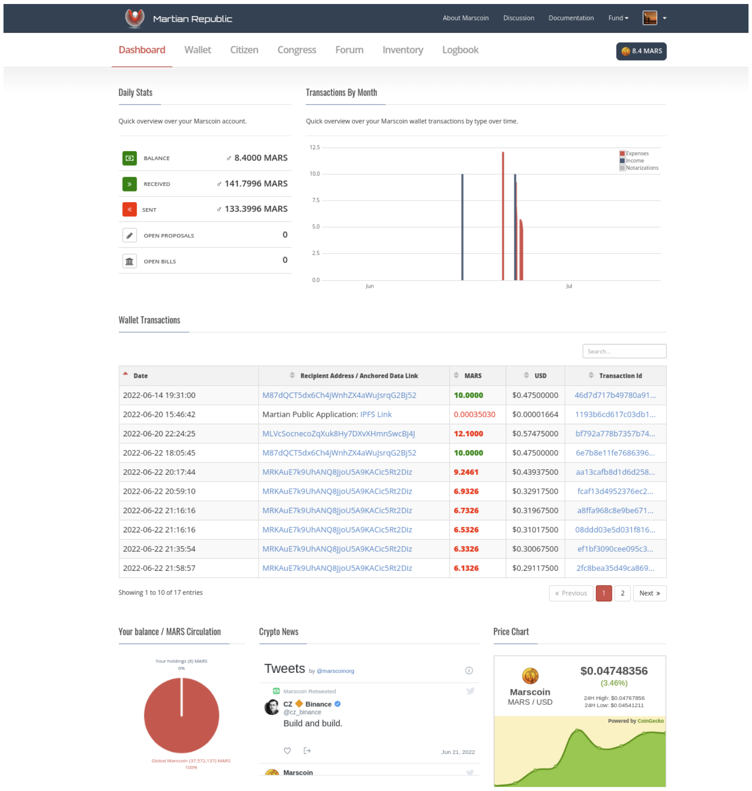
- **Marscoin Wallet** - A non-custodial online HD wallet with built-in encrypted backup service and seed phrase recovery.
- **Martian Citizen** - An on-chain "proof of humanity" peer-based public identity/voter registry using HD Marscoin wallets and decentralized IPFS nodes to store and attest Martian citizenship.
- **Martian Forum** - A HN/Reddit-styled built-in forum to allow proposal and bill discussion for all members of the Martian Republic. Forum entries are regularly notarized via the timestamping and notarization services on-chain to create a censorship-resistant discussion forum.
- **Martian Congress** - An on-chain, ultra-transparent governance system utilizing the non-custodial wallet, public voter registry, and a coin-shuffle-based, encrypted ballot distribution system to ensure fair voting on public proposals, bills, and amendments by secret ballot.
- **Martian Inventory** - Using on-chain tracking of resource production and allocation. An API allows third party (industrial IoT) systems to feed their production results into a Merkle-tree-based timestamping server for transparent inventory tracking.
- **Martian LogBook** - A science log book / blog with on-chain timestamping for recording individual and scientific data in a public format to create an immutable record.
- **Martian Land Registry** - An on-chain registry of land ownership rights. Using the blockchain for notarization and timelocking of funds, the Martian land registry allows users to pre-subscribe to land that the public offers up for sale. The governance of the land rights is tied back into the Martian Congress, allowing the public to ensure public property rights.

3 Marscoin Online Wallet

The Marscoin Online Wallet (”Wallet”) is an open-source non-custodial online hierarchical deterministic (”HD”) wallet with a built-in encrypted backup service and seed phrase recovery.[7]

The wallet serves as the entry point for new users to the transactional features of the Martian Republic and the set of online tools for participation in the civic functions of the Martian colony.

[7] Non-custodial wallets keep the wallet's private keys in the hands of the end user preventing key leakage to third parties [15]. HD wallets follow a Bitcoin specification known as BIP32: [17].



Daily Stats

Quick overview over your Marscoin account.

BALANCE	♂ 8.4000 MARS
RECEIVED	♂ 141.7996 MARS
SENT	♂ 133.3996 MARS
OPEN PROPOSALS	0
OPEN BILLS	0

Transactions By Month

Quick overview over your Marscoin wallet transactions by type over time.

Wallet Transactions

Date	Recipient Address / Anchored Data Link	MARS	USD	Transaction Id
2022-06-14 19:31:00	M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52	10.0000	$0.47500000	46d7d717b49780a91...
2022-06-20 15:46:42	Martian Public Application: IPFS Link	0.00035030	$0.00001664	1193b6cd617c03db1...
2022-06-20 22:24:25	MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J	12.1000	$0.57475000	bf792a778b7357b74...
2022-06-22 18:05:45	M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52	10.0000	$0.47500000	6e7b8e11fe7686396...
2022-06-22 20:17:44	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	9.2461	$0.43937500	aa13cafb8d1d6d258...
2022-06-22 20:59:10	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	6.9326	$0.32917500	fcaf13d4952376ec2...
2022-06-22 21:16:16	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	6.7326	$0.31967500	a8ffa968c8e9be671...
2022-06-22 21:16:16	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	6.5326	$0.31017500	08ddd03e5d031f816...
2022-06-22 21:35:54	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	6.3326	$0.30067500	ef1bf3090cee095c3...
2022-06-22 21:58:57	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	6.1326	$0.29117500	2fc8bea35d49ca869...

Showing 1 to 10 of 17 entries

Your balance / MARS Circulation

Crypto News

Tweets by @marscoinorg

Marscoin Retweeted

CZ 🔶 Binance ✓
@cz_binance
Build and build.

Jun 21, 2022

Marscoin

Price Chart

Marscoin
MARS / USD
$0.04748356
(3.46%)
24H High: $0.04767856
24H Low: $0.04541211

Figure 1: *The dashboard features the wallet summary, transaction list, and Marscoin price charts.*

To setup a wallet a user creates an account on the Martian Republic website (password and 2FA protected by default).[8] Users then create HD wallets in their browser client-side. The website uses random mouse-movements as a strong entropy source to facilitate the generation of a unique secure client-side browser-generated seed phrase.

An AES-encrypted version[9] of the seed phrase thus generated can be backed up server-side. After login, the browser will offer the user to unlock an existing seed phrase to access the wallet. The locked seed phrase is stored in the browser's local storage.

Alternatively, for a more trust-less approach, the wallet can be "loaded" or "reconnected to" by simply re-entering the seed phrase after user login, for those who prefer an extra level of security.

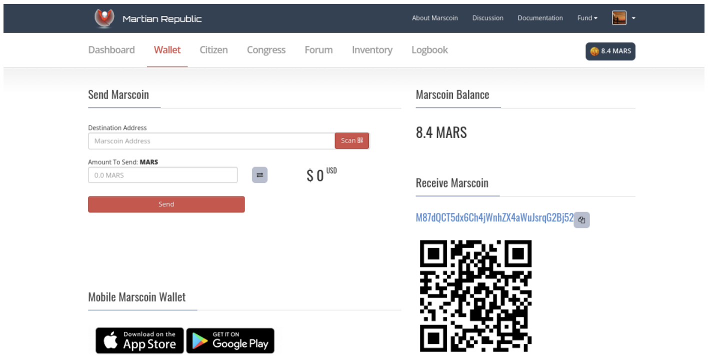
Basic receive and send functions allow users to receive and send Marscoin to and from other participants in the network[10], from the convenience of an online experience and the security of a non-hosted private wallet. The Martian Republic server has no access to the user's private seed

[8] The server login is mainly a feature of the encrypted backup service provided for users. It is not required for the functionality of the Martian Republic which is purely based on private-public key interactions via their wallet and the public Marscoin blockchain.

[9] AES-256 CTR using SHA512 to hash the password prior to encrypting seed phrase. The tool that supplies the cryptographic functionality client-side is the open-source JavaScript library bitcoin-js[8].

[10] By parsing the user's public address balance on-chain and signing any new transactions he intends to spend with his wallet's private key.

phrase[11] or funds at any given point in time.



Send Marscoin

Destination Address: Marscoin Address

Amount To Send: **MARS** 0.0 MARS ⇄ $ 0 USD

Marscoin Balance

8.4 MARS

Receive Marscoin

M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52

Mobile Marscoin Wallet

Figure 2: *Main Non-custodial online wallet view*

The open-source nature allows anyone to vet and improve the online wallet codebase and minimize security risks. It is also intended to allow multiple parties to offer these hosting services and distribute the server load while competing with each other by providing additional services.

As each implementation rests on the blockchain as the ultimate arbiter of truth and the protocol of rules that interpret the blockchain data, various architectures and systems can be deployed that vie for utilization, increasing the decentralized nature of the participating server/client architectures and allowing them to keep evolving.

The Martian Republic wallet currently features two main pages: a Dashboard page with general analytics and the Wallet page itself used for online transactions.

The wallet page features all basic functionality of an online in-browser wallet: The user's Marscoin address is displayed as a string for a quick copy and paste and the QR code available to be scanned by mobile wallets. A scan button allows an active webcam to import any destination addresses. The balance of the wallet is displayed prominently.

4 Martian Citizen

The Martian Citizen Registry is an on-chain "proof of humanity" registry, using decentralized and cryptographically secured metadata and file storage (IPFS + Marscoin) to create a private/public identity attestation system.

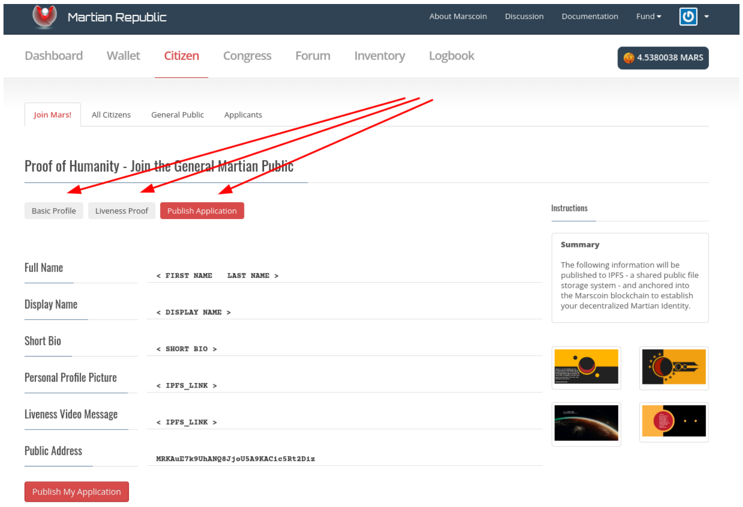
4.1 Joining the General Public

Identity verification systems are key to civic processes. Because of their central importance to all human interactions, they frequently become targets of "attacks." Legacy systems in most nation

[11] A "seed phrase" is a mnemonic equivalent of a private key. It is typically a list of 12 or 24 "random" words [9] and [17].

states consist of massive data silos in national, federal, and private institutions / corporations and often retain an overabundance of data on individuals, violating basic human rights to privacy.

On the other hand, fully decentralized systems that allow member participation without relying on any real-world evidence are vulnerable to Sybil[12] attacks, voter fraud[13][14], and manipulation by third parties.[15]



Proof of Humanity - Join the General Martian Public

Full Name: < FIRST NAME LAST NAME >

Display Name: < DISPLAY NAME >

Short Bio: < SHORT BIO >

Personal Profile Picture: < IPFS_LINK >

Liveness Video Message: < IPFS_LINK >

Public Address: MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz

Summary

The following information will be published to IPFS - a shared public file storage system - and anchored into the Marscoin blockchain to establish your decentralized Martian Identity.

Figure 3: *Profile - Joining the Republic. A minimalistic core set of data that defines a wallet holder as a member of the general public.*

We propose a community-driven identity attestation system in which an initial community outlines the terms of on-boarding new members. Using clear programmatic guidelines and a minimum set of agreed upon personally identifiable information (PII), this system establishes a Public Voter Registry.

This public registry allows members of the community to identify each other cryptographically and securely without giving away any private data they do not intend to share beyond the very basics of the Voter Registry itself. Currently, the three minimal data points upon which this public registry is built, consist of

- A full name and nickname
- A live picture
- A liveness video with evidence of the citizen's civic wallet address (public address)

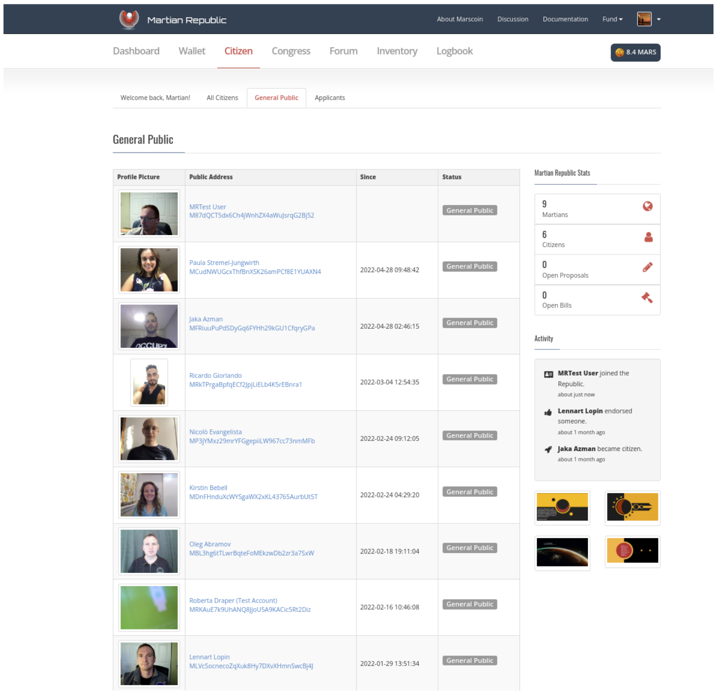
The Martian Republic thus provides a basic user ID including a liveness test, which could be further improved with in-person kiosk-style self-service terminals (for instance upon arrival on Mars) that add a physical component to user onboarding minimizing fraud.

[12] "Exploring sybil and double-spending risks in Blockchain Systems" [6].

[13] Election integrity. Heritage Foundation. [11].

[14] Pew Research Center's Journalism Project. [12].

[15] "DAO Overturns Vote" [14].



General Public

Profile Picture	Public Address	Since	Status
	MRTest User M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52		General Public
	Paula Stremel-Jungwirth MCudNWUGcxThfBnXSK26amPCf8E1YUAXN4	2022-04-28 09:48:42	General Public
	Jaka Azman MFRiuuPuPdSDyGq6FYHh29kGU1CfqryGPa	2022-04-28 02:46:15	General Public
	Ricardo Giorlando MRkTPrgaBpfqECf2JpjLiELb4K5rEBnra1	2022-03-04 12:54:35	General Public
	Nicolò Evangelista MP3jYMxz29mrYFGgepiiLW967cc73nmMFb	2022-02-24 09:12:05	General Public
	Kirstin Bebell MDnFHnduXcWYSgaWX2xKL43765AurbUt5T	2022-02-24 04:29:20	General Public
	Oleg Abramov MBL3hg6tTLwrBqteFoMEkzwDb2zr3a7SxW	2022-02-18 19:11:04	General Public
	Roberta Draper (Test Account) MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	2022-02-16 10:46:08	General Public
	Lennart Lopin MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J	2022-01-29 13:51:34	General Public

Martian Republic Stats

9
Martians

6
Citizens

0
Open Proposals

0
Open Bills

Activity

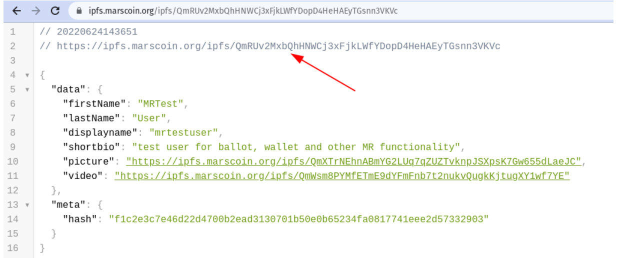
MRTest User joined the Republic.
about just now

Lennart Lopin endorsed someone.
about 1 month ago

Jaka Azman became citizen.
about 1 month ago

Figure 4: *Public Registry - Personally Identifiable Information is limited to a few atomic parameters*

4.2 Safeguarding the Republic



ipfs.marscoin.org/ipfs/QmRUv2MxbQhHNWCj3xFjkLWfYDopD4HeHAEyTGsnn3VKVc

```
// 20220624143651
// https://ipfs.marscoin.org/ipfs/QmRUv2MxbQhHNWCj3xFjkLWfYDopD4HeHAEyTGsnn3VKVc

{
  "data": {
    "firstName": "MRTest",
    "lastName": "User",
    "displayname": "mrtestuser",
    "shortbio": "test user for ballot, wallet and other MR functionality",
    "picture": "https://ipfs.marscoin.org/ipfs/QmXTrNEhnABmYG2LUq7qZUZTvknpJSXpsK7Gw655dLaeJC",
    "video": "https://ipfs.marscoin.org/ipfs/QmWsm8PYMfETmE9dYFmFnb7t2nukvQugkKjtugXY1wf7YE"
  },
  "meta": {
    "hash": "f1c2e3c7e46d22d4700b2ead3130701b50e0b65234fa0817741eee2d57332903"
  }
}
```

Figure 5: *Public Registry - a new user's registration as it appears in the blockchain, confirmed (”notarized”) by the Marscoin blockchain*

After the initial registration, the new “member of the general public” is vetted by the community of existing citizens. Unlike systems in which votes and power are tied to money (one vote per unit of monetary account or acre of land ownership, etc.) favoring the wealthy, influential, early-adopters — or systems, in which opaque and unclear “hidden” legacy databases require trust in a central authority pretending to “manage” the legitimacy of individuals participating in society (i.e. state database for driver's licenses or voter registrations maintained by appointed yet unelected officials) the Martian Republic's Public Registry crowd-sources the trustworthiness of its citizen database via transparent and immutable ledger entries[16].

One of the most basic civic duties of each Martian citizen thus includes simply checking new and old entries in the public registry for fraudulent or attempted duplicate entries. Citizens will decide as a group how many endorsements or delisting-votes a record needs before it becomes either a valid citizen or is allowed to be removed ("*exile*"), minimizing abuse in both directions and transparently defining and streamlining on-boarding ("*immigration*") policies as basic rules written into the code of the Martian Republic itself. The built-in and readily available voting system provides an "immune system" for the *body politic* of the governed who standardize and enforce the expression of their sovereign intent succinctly by virtue of programmatic procedures. Additionally, it helps their society avoid "parasitic capture" by groups that might otherwise undermine or co-opt complex authority-only and centralized, trust-based communication processes or ambiguously interpret legal proceedings.

4.3 Becoming Citizen

Once a new registrant's identity has been established and his profile added to the "proof of humanity" database or Public Registry, existing citizens can start to vouch for the individual. The data for each user (a basic JSON[17] data structure - see fig. 5) lives decentralized in a global IPFS[18] cloud of file servers, which constantly replicate and cache this information and make sure that it is readily available planet-wide.

During the registration process, this "atomic" (identity describing) JSON data object is SHA265 hashed and its hash inserted into the Marscoin blockchain. It thus becomes clearly and permanently linked to the citizen's public/civic Marscoin address.[19]

Once an applicant's data has thus been successfully "notarized", i.e after the broadcasted small transaction containing his public data set has been confirmed on the Marscoin blockchain, any Martian Republic's server will list the new applicant as a member of the *General Public.*

This identity record is now available on-chain and can be consumed and re-displayed by other members of the community replacing the traditional concept of "passport" of nation states (see fig. 8).

To elevate one's privileges in the system further to that of "citizen" with voting rights, a member of the General Public has to receive 1 endorsement per 10 citizens total. In the current implementation we cap the minimum endorsements required at five when the number of citizens exceeds fifty citizen users total.[20]

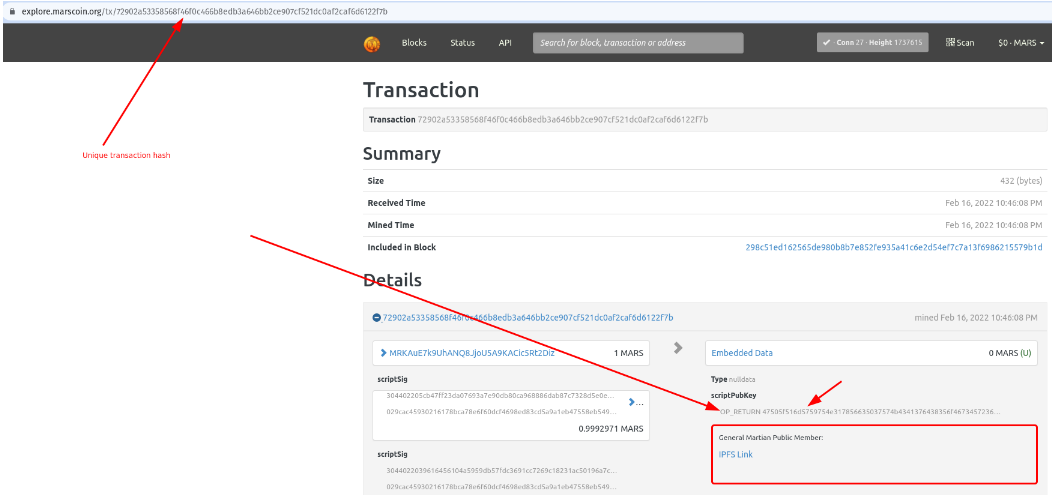
[16] In case of lost private keys existing citizens need to open a new account. The citizenry will define very clear specifications what a shift of an existing citizen to a new address entails ("re-naturalization" or "citizenship verification"). Streamlined procedures under the watchful eyes of existing citizens would provide clear pathways to re-acquire one's (temporarily inaccessible) citizenship status.

[17] JavaScript Object Notation. [13]

[18] IPFS is a distributed system for storing and accessing files, websites, applications, and data. Making it possible to download a file from many locations that aren't managed by one organization supports a resilient internet, makes it harder to censor content and can speed up the web when being far away or disconnected. See `https://docs.ipfs.io/concepts/what-is-ipfs/` for more information.

[19] Users can maintain any number of wallets for all kinds of different purposes, but will be required to use one public address, tied to their Public Registry, for all their civic interactions that require identity verification.

[20] Rules like these make up the basic configuration - Constitution - of the Republic and should be voted upon for updates, requiring the highest level of participation and thresholds to pass. As a recursive and "living" organism, even these considerations can be clearly discussed on public forums and brought to vote by other citizens. Thus the formation of ad-hoc voting blocks, parties, temporarily executive leaders, etc. are all within the flexible bounds of


Unique transaction hash
Blocks
Status
API
Search for block, transaction or address
✓ · Conn 27 · Height 1737615
Scan
$0 · MARS

explore.marscoin.org/tx/72902a53358568f46f0c466b8edb3a646bb2ce907cf521dc0af2caf6d6122f7b

Transaction

Transaction 72902a53358568f46f0c466b8edb3a646bb2ce907cf521dc0af2caf6d6122f7b

Summary

Size	432 (bytes)
Received Time	Feb 16, 2022 10:46:08 PM
Mined Time	Feb 16, 2022 10:46:08 PM
Included in Block	298c51ed162565de980b8b7e852fe935a41c6e2d54ef7c7a13f6986215579b1d

Details

72902a53358568f46f0c466b8edb3a646bb2ce907cf521dc0af2caf6d6122f7b mined Feb 16, 2022 10:46:08 PM

MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz 1 MARS

scriptSig
304402205cb47ff23da07693a7e90db80ca968886dab87c7328d5e0e...
029cac45930216178bca78e6f60dcf4698ed83cd5a9a1eb47558eb549...

0.9992971 MARS

scriptSig
3044022039616456104a5959db57fdc3691cc7269c18231ac50196a7c...
029cac45930216178bca78e6f60dcf4698ed83cd5a9a1eb47558eb549...

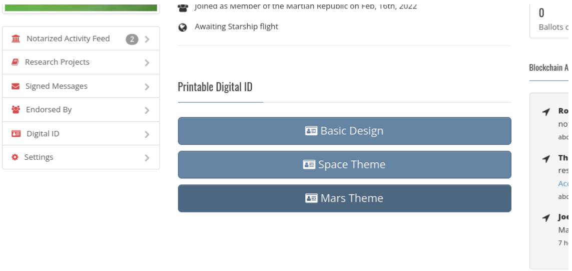
Embedded Data 0 MARS (U)

Type nulldata

scriptPubKey
OP_RETURN 47505f516d5759754e317856635037574b4341376438356f4673457236...

General Martian Public Member:
IPFS Link

Figure 6: *A user became member of the general public. Transaction recorded on blockchain. The OP_RETURN hex value contains an ASCII-encoded IPFS link.*



Joined as Member of the Martian Republic on Feb, 16th, 2022

Awaiting Starship flight

Printable Digital ID

Figure 7: *Profile - Citizen's Digital ID*

When a member of the General Public passes the threshold of endorsements, their status is automatically upgraded to citizen and they will be able to participate in the next proposal vote.

How does the Martian Republic know about status changes? As all notarizations occur publicly on the blockchain, any participant of the Martian Republic can verify that a particular member has received the number of endorsements required for citizenship.[21]

Typically this job will be done by transaction parsing tools. One of these is included in the Martian Republic's open source code repository. As it is open source, new transaction data types can be added and new structures and rules can be embedded in the blockchain over time.[22]

the Martian Republic design – however always fall under actionable public scrutiny.

[21] Bad actors, individuals or machines face bans and rejection from the network of "constitutional peers".

[22] The data structures added to the blockchain are miniscule and could be combined in Merkle trees. We do not forsee this extra data to become a limiting factor on the data storage needs of a blockchain like Marscoin. In fact it promotes mining activity even long after the mining rewards have ceased to present any reasonable incentive for miners who are needed to protect the network against 51% attacks. A virtuous circle between miners, blockchain and civic platform.

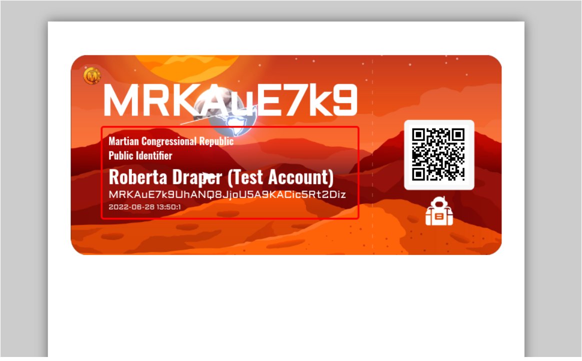

MRKAuE7k9
Martian Congressional Republic
Public Identifier
Roberta Draper (Test Account)
MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz
2022-06-28 13:50:1

Figure 8: *Citizen's Digital ID turned "passport"*

4.4 Civic Activities

While citizens participate in activities on the Martian Republic, open-source background scripts analyze all incoming transactions and identify civic transactions. These Marscoin transactions which contain certain embedded flags in their OP_RETURN[23] are then analyzed and cached locally - As all data is transparent and in the public domain, anyone can easily verify that the agreed-upon rules are being followed.[24]

Any activities that do not require official notarization but are private in nature can just be performed from a wallet that the user also owns but does not link to their citizenship and voter registry entry.

5 Martian Forum

The Martian Forum is a Reddit/Hackernews style built-in forum that allows proposal and bill discussions for all members of the Martian Republic. Forum entries will be regularly notarized via a timestamping and notarization service to prevent tampering with messages and to ensure free speech expression for all participants.

It is quite apparent that all political and governance processes that the Martian Republic attempts to manage demand a public forum for open discourse. When all discussions pertaining to changes and additions are kept on record and find a central safe place for future reference, the Republic's development becomes a story written by its members.

The desire to avoid third party community tools (Discord, Facebook, Twitter, etc.) and allow for easy reference of community discussions in proposals submitted to society at large, led to the

[23] for example: *ED* ... Endorsement, *PR* ... Proposal, *SP* ... Signed Message, PRY ... Vote yes on proposal. These flags are followed by an underscore and the respective IPFS identifier. To wit OP_RETURN 53505f516d555878355a63715155397553546b43714d6850674648675072684c324567566d4554444543373368 34586b4c (hex) translates to SP_QmUXx5ZcqQU9uSTkCqMhPgFHgPrhL2EgVmETDEC73h4XkL (ascii). Using an IPFS web link and navigating to `https://ipfs.marscoin.org/ipfs/QmUXx5ZcqQU9uSTkCqMhPgFHgPrhL2EgVmETDEC73h4XkL` allows us to look up the data set that was notarized by the Marscoin blockchain and stored in the IPFS file storage network.

[24] Election results, for instance, will not include votes cast by public addresses that lack full citizenship endorsements.

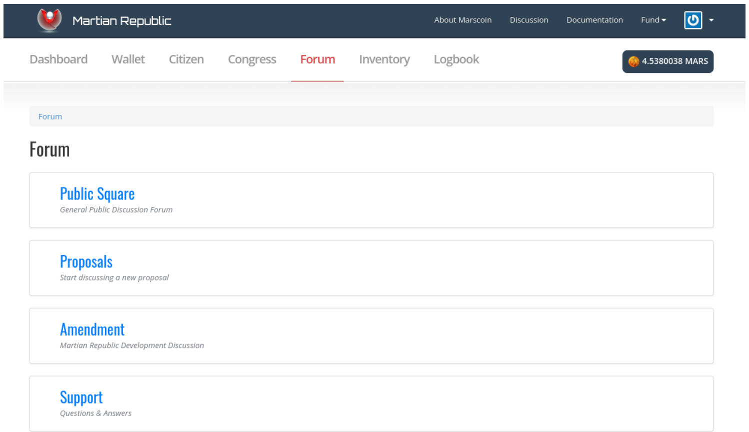


Figure 9: *The Forum*

design of the Martian Forum[25].

It is intended to be the default location for public discussions on new proposals and allows citizens to refer to historic proposals. Hashed timestamps referencing forum discussions encourage the development of a transparent and censor-resistant place for all members of the public. The decision to refer to users via their public citizen address intends to create an atmosphere of mutual respect and individual participation[26]. This design philosophy of the Martian Republic aligns itself with ideals of the early Roman and the American Republic in which each citizen carries full responsibility and considers participation an honorary involvement. However, the decentralized nature of wallets and memberships *do* allow indeed throw-away accounts that could participate in discussions as well.

Achieving substantial discussions on various topics and not having to worry about shadow-banning, content manipulation or other curtailing of free speech is one of the defining goals of the forum. With the source code of the Martian Forum being part of the very Constitution of the Martian Republic, it stands to reason that the informed majority will uphold free speech.

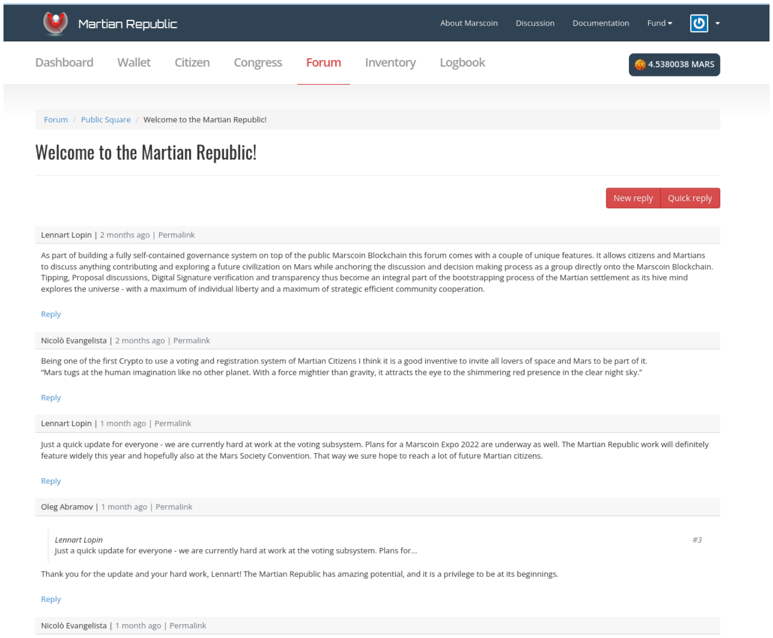
6 Martian Congress - Decentralized Public Governance

The "Congress" section of the Martian Republic builds on the various modules discussed thus far. The ability to present ideas in a forum among peers, to put suggestions up for vote with outcomes that (in a cryptographically-secured process) ensure the expression of society, to build on pre-established principles or modify them when necessary — all this creates a unified and organized group of individuals who are able to tackle ever-increasing complex public problems from first principles.[27] The crucial point however is that the trust of the individual in the decision making

[25] E.g. a proposal submission automatically generates a new discussion thread in the Proposal section of the Martian Forum

[26] "How facebook's real-name policy changed Social Media Forever"[10].

[27] In a rare display of deep understanding of economic and indeed civilizational first principles, Irwin A. Schiff so aptly portraits in his book "How an economy grows and why it doesn't"[16] the power and plight of a community of people who – through an unbiased medium of exchange – either coordinate their forces against a hostile entropic



Welcome to the Martian Republic!

Lennart Lopin | 2 months ago | Permalink

As part of building a fully self-contained governance system on top of the public Marscoin Blockchain this forum comes with a couple of unique features. It allows citizens and Martians to discuss anything contributing and exploring a future civilization on Mars while anchoring the discussion and decision making process as a group directly onto the Marscoin Blockchain. Tipping, Proposal discussions, Digital Signature verification and transparency thus become an integral part of the bootstrapping process of the Martian settlement as its hive mind explores the universe - with a maximum of individual liberty and a maximum of strategic efficient community cooperation.

Reply

Nicolò Evangelista | 2 months ago | Permalink

Being one of the first Crypto to use a voting and registration system of Martian Citizens I think it is a good inventive to invite all lovers of space and Mars to be part of it.
"Mars tugs at the human imagination like no other planet. With a force mightier than gravity, it attracts the eye to the shimmering red presence in the clear night sky."

Reply

Lennart Lopin | 1 month ago | Permalink

Just a quick update for everyone - we are currently hard at work at the voting subsystem. Plans for a Marscoin Expo 2022 are underway as well. The Martian Republic work will definitely feature widely this year and hopefully also at the Mars Society Convention. That way we sure hope to reach a lot of future Martian citizens.

Reply

Oleg Abramov | 1 month ago | Permalink

> *Lennart Lopin* *#3*
> Just a quick update for everyone - we are currently hard at work at the voting subsystem. Plans for...

Thank you for the update and your hard work, Lennart! The Martian Republic has amazing potential, and it is a privilege to be at its beginnings.

Reply

Nicolò Evangelista | 1 month ago | Permalink

Figure 10: *Forum posts and response*

process of the community hinges upon trust in the voting process itself.[28] Applying the idea of "Trust, but verify", we propose a novel end-to-end auditable voting process.

6.1 Implementation of secure voting

Goals of an end-to-end auditable and secure electronic voting process are as follows:

- Correctness:
  - Only authorized parties can vote, i.e. registered voters
  - No voter votes more than once
  - No voter can replace votes
  - The party in charge of tabulation cannot change the outcome
- Verifiability: universal and private
- User anonymity
- Receipt-freeness

universe and achieve an incredible level of cultural and technological progress or fail in the process by abusing the very foundation of their cooperation. Stored and easily accessible energy is a force of life - not just for the highly sophisticated organism but also for any other individual or group that is allowed access only to waste it – an entropic lightning rod, of sorts [18] [20].

[28] "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 in [22].

We achieve these goals using a combination of a freely and publicly available online wallet, a citizen registry with "proof-of-humanity", a private and secret coin-shuffle-based ballot acquisition procedure and finally with a proposal platform that allows proposals to be timestamped and anchored in a public blockchain (Marscoin) for immutability and verifiability.

6.2 Overview

After a user successfully registered an account in the public user registry using his private and secure online citizen wallet furnishing a "proof of humanity" to the body of the citizenry, the new member awaits enough endorsements (votes of confidence) from existing citizens. Once a certain threshold of community members vouch for the user and elevate him to the status of citizen, the citizen thus becomes allegeable to join the proposal and voting process.

Any citizen can create their own proposal. Each proposal consists of a title, a description and parameters regarding the voting process. The proposal once published (*IPFS*) will be notarized by the Marscoin blockchain. In the current implementation, all proposals posted are open for the public vote. A citizen can check out new active proposals, discuss them in the public *Forum* and then proceed to request a ballot and cast a vote on the proposal. If the proposal does not garner enough votes in the allotted time (percentage threshold missed), it simply fails but will nevertheless appear in the "congressional archive".

Voting on existing proposals requires the receipt of a ballot. A ballot is simply a small unit of Marscoin (0.1 MARS at the moment[29] which a user receives after participating in a ballot-shuffle. The underlying coin-shuffle allows us to cryptographically establish a private vote that is auditable yet private. To participate in a vote, a citizen joins the ballot shuffle.

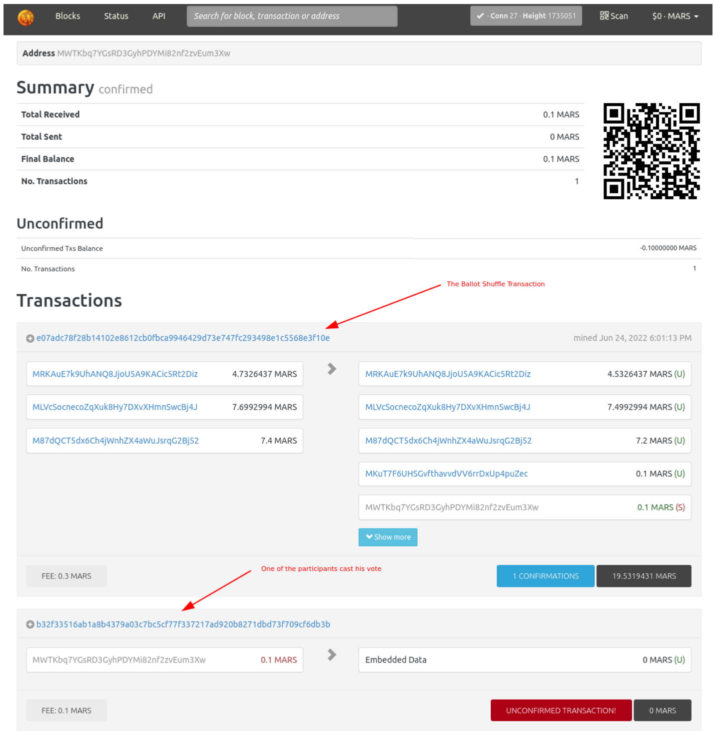
The shuffle creates a transaction in which all participants receive their 0.1 MARS coin returned on a newly generated Marscoin address with zero prior history. While the participants in the coin-shuffle are on-chain – and verifiably participants from among the voter registry (identified by their public Marscoin address) – the 0.1 MARS ballot which the coin-shuffle returned *cannot* be traced back to any individual voter as such. Such private ballot, i.e. a 0.1 MARS balance on the freshly funded new Marscoin address is then *"cast"*[30] by forming a new transaction confirming the citizen's voting intention. It shows up on the blockchain visibly derived from a pool of citizens but cannot be linked to any one of them individually.

Ballot shuffles take place frequently and are automatically generated on the server using websocket connections from (citizen) client wallets requesting new ballots. This ensures that all important parts of the system are independently verifiable and visible on-chain, establishing an end-to-end auditable voting system:

- A citizen is identified by his public address.
- A citizen's public address appears in a ballot-requesting ("coin-shuffle") transaction with a set of target addresses ("ballots").

[29] 1 MARS (Marscoin) equals 100,000,000 zubrin - we launched the Martian Republic with a ballot commitment of 10,000,000 zubrin or 0.1 Marscoin. This amount is a great example of configuration settings that the public can adjust. Preventing spamming on the one hand but making voting a very affordable but still a small monetary commitment (comparable to paying for gas driving to a polling station or fractions thereof) increases the weight of the vote and supports the miners in securing the blockchain.

[30] or *"burnt"* as the funds will be completely spent in the vote and thus benefit the miners who secure the network.



Address MWTKbq7YGsRD3GyhPDYMi82nf2zvEum3Xw

Summary confirmed

Total Received	0.1 MARS
Total Sent	0 MARS
Final Balance	0.1 MARS
No. Transactions	1

Unconfirmed

Unconfirmed Txs Balance	-0.10000000 MARS
No. Transactions	1

Transactions

The Ballot Shuffle Transaction

e07adc78f28b14102e8612cb0fbca9946429d73e747fc293498e1c5568e3f10e — mined Jun 24, 2022 6:01:13 PM

MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	4.7326437 MARS	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	4.5326437 MARS (U)
MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J	7.6992994 MARS	MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J	7.4992994 MARS (U)
M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52	7.4 MARS	M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52	7.2 MARS (U)
		MKuT7F6UHSGvfthavvdVV6rrDxUp4puZec	0.1 MARS (U)
		MWTKbq7YGsRD3GyhPDYMi82nf2zvEum3Xw	0.1 MARS (S)

FEE: 0.3 MARS — 19.5319431 MARS

One of the participants cast his vote

b32f33516ab1a8b4379a03c7bc5cf77f337217ad920b8271dbd73f709cf6db3b

MWTKbq7YGsRD3GyhPDYMi82nf2zvEum3Xw	0.1 MARS	Embedded Data	0 MARS (U)

FEE: 0.1 MARS — 0 MARS

Figure 11: *The ballot shuffle transaction and a subsequent citizen's vote*

- The returned shuffle-secured and private *"ballot-coins"* are visible on-chain as well.

- The transactions signed with these coins containing the voting intent are clearly visible as well.

- The vote tally is a sum of all these signed ballot-coins (with embedded vote metadata) transacted on the blockchain.

Citizens are free to cast their vote on the proposal for which the ballot shuffle process originated a secret ballot. Ballots are not re-usable and can't be spent on other proposals. Any interference in the ballot shuffle process by bad actors could lead to that individual's (temporary banning).[31] Rules thus enshrined as software to facilitate a fair election process on a programmatic level are likely to develop further and become more sophisticated over time.

The 0.1 MARS spent on the vote is "burnt" - no change address is being provided which means that the ballot transaction becomes a miner fee subsidizing the miners securing the network which in turn helps citizens record their decision privately and tamper-proof. No coins are lost in the process. **The miners get paid for supporting not only the financial backbone of the colony but also the governance system**.

[31] The ballot shuffle does require an online presence for coordination with the ballot server. A mobile app version could be a useful complementary alternative to the current browser only implementation and make it easier to receive secret ballots "on the go".

Using a highly ASIC-resistant algorithm we propose that most citizens would also run their own mining nodes.[32]

The server script then tallies the publicly visible blockchain-notarized votes and highlights the results for convenience on the Martian Republic platform - links to block-explorers allow any citizen to verify these results personally. As the voting occurs completely transparently on-chain, a verification is possible by anyone without the need for sophisticated tools or other indirect assessments: The Martian Republic's design was intended to create a system that avoids opaqueness, obfuscation and unnecessary complexity as much as possible.

6.3 Proposal

While different types of proposals govern different aspects of this citizen-driven direct congressional republican government the base upon which the system is built becomes our **"Constitution"**: the code and configuration settings underlying the Martian Republic. The code on which the system runs is itself stored as open source in a public repository. Daily *git pulls*[33] are hashed and inserted into the Marscoin blockchain allowing anyone to see that the current version of their "government" is *de facto* the one they are operating on. Any proposals that suggest changes to the very codebase are first order proposals, i.e. "amendments" and take the most effort to go into effect.

6.4 Creating proposals

When a proposal is submitted via the proposal editor the proposal parameters are distributed via the IPFS mesh network. The IPFS link is then timestamped via another data-embedded Marscoin transaction. This also exposes the new proposals to any other nodes/servers that watch the Marscoin blockchain and might offer up this information to other decentralized participants of the Martian Republic (which, after all, is more a protocol based on top of a blockchain. Our implementation can be seen as an instantiation of this ephemeral rule-set that's evolving on the trustless Marscoin ledger).

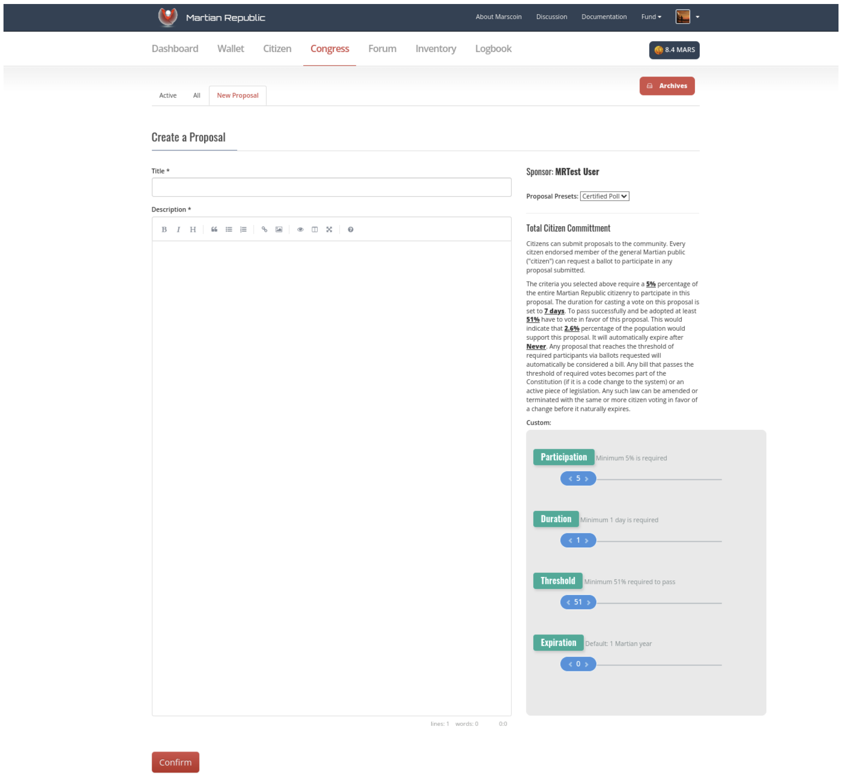
A proposal is defined by title and description and voting configuration preset. The new proposals could include a new piece of code, patch, amendment, rule change, declaration, law, etc. Selecting from a drop-down the proposal voting presets are pre-selected. This impacts a series of parameters which can also be fine-tuned further.

Each preset comes with a *"total citizen commitment"* specifying the proposal constraints. The more restrictive the various parameter thresholds the more weight a proposal carries. While some proposals might be actual code changes, others could just express an intent of the community. However all non-code proposals have a built-in expiration date to insure that regulations do not become overly burdensome over time.[34]

[32] For instance via proposals to move the Marscoin blockchain from scrypt-mining to RandomX (RandomX is a proof-of-work (PoW) algorithm that is optimized for general-purpose CPUs. RandomX uses random code execution (hence the name) together with several memory-hard techniques to minimize the efficiency advantage of specialized hardware. `https://github.com/tevador/RandomX`. This would greatly democratize the blockchain support, and increase security to prevent 51% attacks, and allow many computing devices to "background mine" when idle. Given the importance of using their Marscoin blockchain for decentralized finance and governance, the future Martians would eagerly pursue a course that takes these important public activities out of the purview of any small minority.

[33] The git pull command is used to fetch and download content from a remote repository and update a local codebase and match any changes.

[34] "I think I would recommend some adjustment for the inertia of laws would be wise. It should probably be easier



Create a Proposal

Title *

Description *

Sponsor: **MRTest User**

Proposal Presets: Certified Poll

Total Citizen Committment

Citizens can submit proposals to the community. Every citizen endorsed member of the general Martian public ("citizen") can request a ballot to participate in any proposal submitted.

The criteria you selected above require a **5%** percentage of the entire Martian Republic citizenry to partcipate in this proposal. The duration for casting a vote on this proposal is set to **7 days**. To pass successfully and be adopted at least **51%** have to vote in favor of this proposal. This would indicate that **2.6%** percentage of the population would support this proposal. It will automatically expire after **Never**. Any proposal that reaches the threshold of required participants via ballots requested will automatically be considered a bill. Any bill that passes the threshold of required votes becomes part of the Constitution (if it is a code change to the system) or an active piece of legislation. Any such law can be amended or terminated with the same or more citizen voting in favor of a change before it naturally expires.

Custom:

Participation Minimum 5% is required
5

Duration Minimum 1 day is required
1

Threshold Minimum 51% required to pass
51

Expiration Default: 1 Martian year
0

Figure 12: *The proposal editor*

Let's take an example. In the case of selecting the preset "Law" the *total citizen commitment* explains:

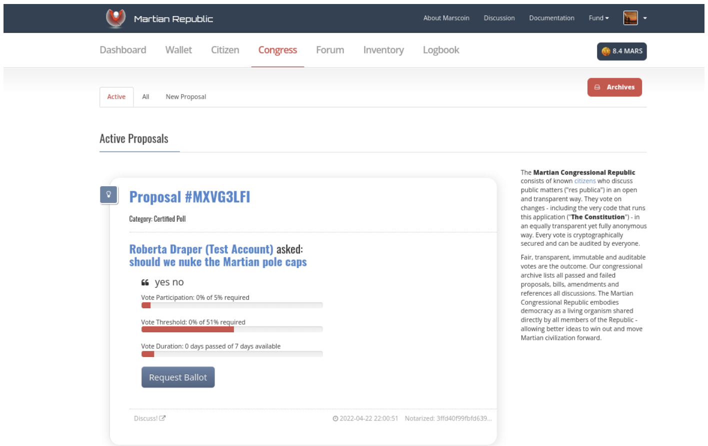
> *The criteria you selected above require a 80% of the entire Martian Republic citizenry to participate in this proposal. The duration for casting a vote on this proposal is set to 30 days. To pass successfully and be adopted at least 65% have to vote in favor of this proposal. This would indicate that 52% of the population would support this proposal. It will automatically expire after 2672 sols (4 years). Any proposal that reaches the threshold of required participants via ballots requested will automatically be considered a bill. Any bill that passes the threshold of required yay votes becomes part of the Constitution (if it is a code change to the system) or an active piece of legislation. Any such law can be amended or terminated before it naturally expires.*

The main parameters are run-time of the bill and its necessary minimum threshold of affirmative votes. These parameters are not set individually but determined by the Constitution ("source code") which itself is open to further discussion and modification.

to remove a law than create one," said Musk. "I think that's probably good, because laws have infinite life unless they're taken away." He also argued that all laws should have a built-in sunset provision — a clause that basically establishes an expiration date for the law unless it's approved again. "If it's not good enough to be voted back in, maybe it shouldn't be there," said Musk.[5]

Thus the citizens are in full control of their own governance system[35]: They explore ideas via the forum, they make various proposals and try to garner support for these. Any code changes are actual software pull requests (*"patches"*) that get merged back into the codebase (the Martian *"Constitution"*) and become effective with the next automated reboot of the system. If these are simply rules, laws, regulations they appear in the archive after being voted upon as "active legislation" (including origination date, expiration date and voting and forum history with an easy way to reference them by permalinks).[36]

Once a proposal gets submitted, the proposal creator is asked to fund the proposal notarization transaction from his wallet (a small Marscoin amount prevents someone from spamming the system). The current version of the Martian Republic requires 1 MARS fee.[37] Upon successful submission the Martian Republic automatically generates a forum entry in the "Proposal" discussion section with the name of the particular proposal.



Proposal #MXVG3LFI

Category: Certified Poll

Roberta Draper (Test Account) asked:
should we nuke the Martian pole caps

yes no

Vote Participation: 0% of 5% required

Vote Threshold: 0% of 51% required

Vote Duration: 0 days passed of 7 days available

2022-04-22 22:00:51 Notarized: 3ffd40f99fbfd639...

The **Martian Congressional Republic** consists of known citizens who discuss public matters ("res publica") in an open and transparent way. They vote on changes - including the very code that runs this application ("**The Constitution**") - in an equally transparent yet fully anonymous way. Every vote is cryptographically secured and can be audited by everyone.

Fair, transparent, immutable and auditable votes are the outcome. Our congressional archive lists all passed and failed proposals, bills, amendments and references all discussions. The Martian Congressional Republic embodies democracy as a living organism shared directly by all members of the Republic - allowing better ideas to win out and move Martian civilization forward.

Figure 13: *Open proposal. Ready to request a ballot and cast a vote.*

[35] The period of early American Republicanism offers a fascinating insight into group dynamics when locked up economic and political interests held by smaller groups of people (aristocracy) suddenly get released by (direct) democratic processes. See "Empire of Liberty", chapters 1-2 for a detailed discussion on positive and negative aspects to be expected by full self-governance and frequent voting [19].

[36] A bill is a proposal that has reached the minimum threshold of citizens participating in voting on said proposal. In order for the bill to become adopted, it has to pass the threshold of yeas versus nays. Bills that passed as well as those that were rejected enter the Martian Republic archives for future reference.

[37] 1MARS = 0.04 USD at the time of publishing. Decentralized cryptocurrencies like Marscoin fluctuate based on supply and demand. With wide-spread adoption these price fluctuations are expected to decrease [21].

6.5 Ballot

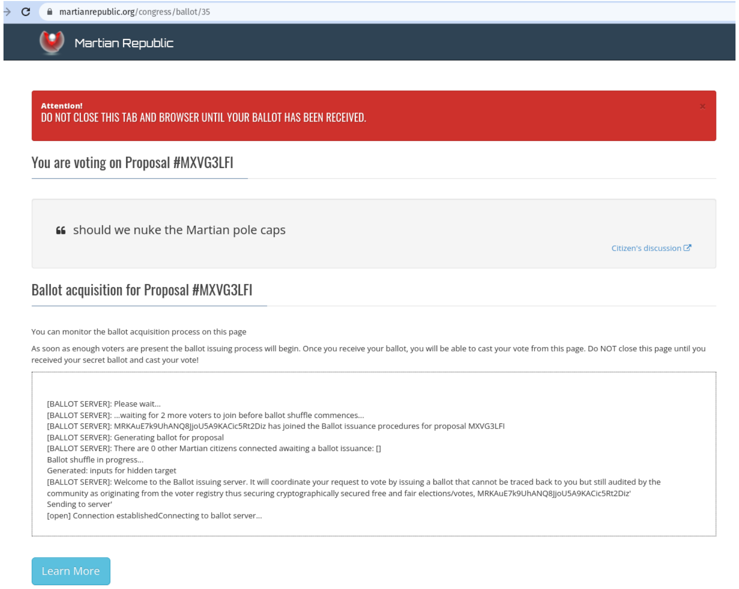
6.5.1 Prerequisites and ballot acquisition

Each member of the Citizen's registry (*"voter registry"*) is afforded one ballot per proposal vote. Each citizen is equally invited to submit new proposals. Proposal categories come with different *"periods"* (days a proposal can be voted on) and different percentage hurdles they have to take in order to be formally adopted ("*threshold*").

A proposal to remove a previous law for instance has a lower threshold than a proposal to create a new law. Special forms of a proposal like constitutional amendments and system code changes require higher participation and percentage thresholds than simple guidelines or community motions. Once a proposal has enough participants (citizens who requested a ballot) it becomes automatically a bill. In order to cast a vote on a bill within its active voting period, a citizen has to request a ballot.

6.5.2 Behind the scenes

Imagine a virtual polling station that waits until it gets a batch of 50 citizens with open ballot requests (this number could be higher or lower depending on number of overall citizens in the systems and desired level of anonymity). As soon as the 50th citizen enters this virtual polling station every participant's browser starts encrypting and shuffling transaction inputs from which they derive - alltogether - a new joint transaction in which all incoming transactions clearly belong to citizens as identifiable via the Voter Registry but whose outputs are all mixed up and thus not traceable back to any individual.



Attention!
DO NOT CLOSE THIS TAB AND BROWSER UNTIL YOUR BALLOT HAS BEEN RECEIVED.

You are voting on Proposal #MXVG3LFI

should we nuke the Martian pole caps

Ballot acquisition for Proposal #MXVG3LFI

You can monitor the ballot acquisition process on this page

As soon as enough voters are present the ballot issuing process will begin. Once you receive your ballot, you will be able to cast your vote from this page. Do NOT close this page until you received your secret ballot and cast your vote!

```
[BALLOT SERVER]: Please wait...
[BALLOT SERVER]: ...waiting for 2 more voters to join before ballot shuffle commences...
[BALLOT SERVER]: MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz has joined the Ballot issuance procedures for proposal MXVG3LFI
[BALLOT SERVER]: Generating ballot for proposal
[BALLOT SERVER]: There are 0 other Martian citizens connected awaiting a ballot issuance: []
Ballot shuffle in progress...
Generated: inputs for hidden target
[BALLOT SERVER]: Welcome to the Ballot issuing server. It will coordinate your request to vote by issuing a ballot that cannot be traced back to you but still audited by the
community as originating from the voter registry thus securing cryptographically secured free and fair elections/votes, MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz'
Sending to server'
[open] Connection establishedConnecting to ballot server...
```

Figure 14: *The "polling station" - the shuffle process generating a private secure ballot.*

The shuffle itself can take a few seconds to a few minutes depending on participation size. When it completes, every participating voter in this virtual polling station page will see a message that their new secret ballot is currently pending confirmation on the blockchain[38]. A few minutes later, large Yes/No/Abstain buttons appear. At this point the citizen can safely vote, spending (*"burning"*) a tiny amount of Marscoin. This transaction gets mined by the miners of the Marscoin network who thus confirm and notarize the (cryptographically secured and thus immutable[39]) vote itself. The transaction that enshrines the vote is a data-embedded Marscoin blockchain transaction.

Meanwhile, our open source tools that track all data transactions as they appear on the Marscoin blockchain see the various votes stream in and are able to tally them up -but won't be able to infer who cast which vote. Everyone is able to see that those votes originated from a ballot shuffle with known, legitimate, Martian citizens - but nobody can attribute a particular vote to a particular individual. A fair, end-to-end auditable, on-chain and thus easily verifiable election took place.

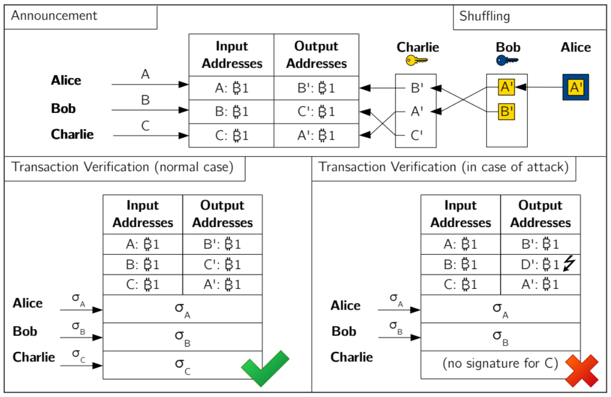


Fig. 2. Overview of CoinShuffle: First, the participants announce their input addresses. Second, they perform a shuffling of fresh output addresses. (Colored boxes represent ciphertexts encrypted with the respective encryption key.) Third, the participants check if their output address is contained in the final list of output addresses. In this case (left-hand side), the transaction is signed by the participants and submitted to the Bitcoin network. If, on the contrary, an output address is missing (e.g., C' has been replaced by D', right-hand side), the transaction does not become valid and the participants enter the blame phase to find out which participant deviated from the protocol specification.

Figure 15: *Overview of a CoinShuffle [7]*

Ballots are requested by browsing the Congress section of the Martian Republic and selecting any of the open proposals or ongoing bills that are of interest. Due to the nature of the ballot-shuffle a citizen's browser has to be online at the time of the shuffle. The minimum number of ballot shuffle participants is technically three -but the more are participating the harder it is for anyone to infer voting behavior from the citizens participating. We assume that this "virtual polling station minimum" of citizens needed to initiate a ballot shuffle will be a function of the number of citizens in the system and be part of the overall Martian Republic Constitution or "settings". As many groups of citizens could request ballots in parallel and the client/server architecture allows for easy scaling the only bottleneck could be the Marscoin blockchain which would have to deal with confirmations of 10,000s of transactions (50 citizens each) over the span of a day in case of

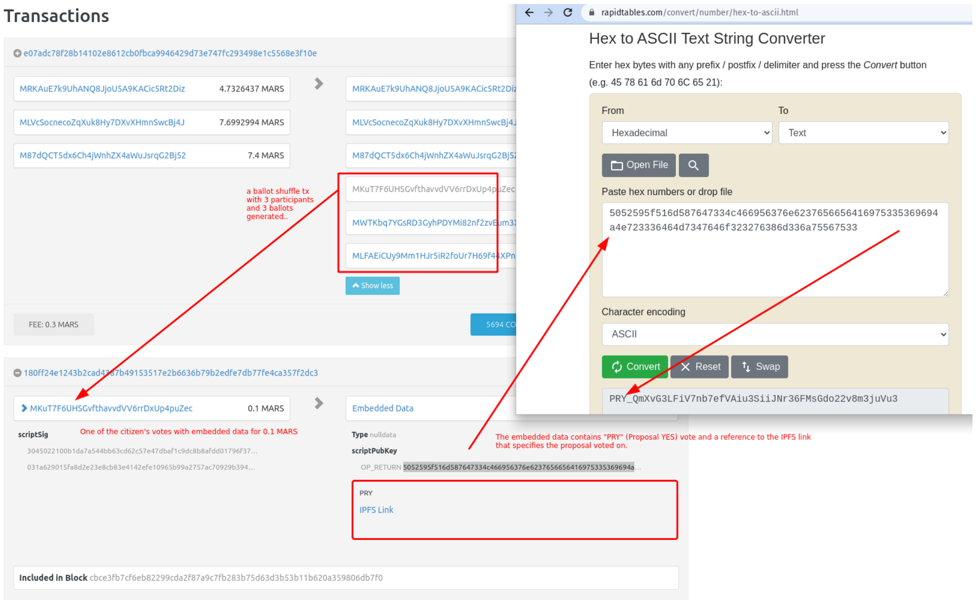
[38] Marscoin's average confirmation time is 2 minutes

[39] "Eternity Wall" is a project that records messages on the Bitcoin blockchain. While not used for governance functions, it has become a central reference point for decentralized messages on Earth's blockchain, Bitcoin. `https://eternitywall.it/`

more important bills. But even here, future voting blocks, Merkle-tree designs and other creative solutions might elevate any bottlenecks.

After clicking the *"request ballot"* button and thus entering the *"virtual polling station"* the citizen simply leaves a browser tab open. The browser-built in websocket will co-ordinate the allocation of 0.1 MARS from its citizen wallet and form a new private ballot address client-side. Once the ballot shuffle is finished, citizens are presented with options to vote. Casting a vote will turn the user's choice into a signed transaction which gets broadcasted to the Marscoin network and turned into a confirmed vote on-chain.

Looking at a vote transaction on the Marscoin blockchain shows a cast vote as one of the following OP_RETURNS:



Transactions

e07adc78f28b14102e8612cb0fbca9946429d73e747fc293498e1c5568e3f10e

MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz	4.7326437 MARS	›	MRKAuE7k9UhANQ8JjoU5A9KACic5Rt2Diz
MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J	7.6992994 MARS		MLVcSocnecoZqXuk8Hy7DXvXHmnSwcBj4J
M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52	7.4 MARS		M87dQCT5dx6Ch4jWnhZX4aWuJsrqG2Bj52
			MKuT7F6UHSGvfthavvdVV6rrDxUp4puZec
			MWTKbq7YGsRD3GyhPDYMi82nf2zvEum3X
			MLFAEiCUy9Mm1HJr5iR2foUr7H69f44XPn

a ballot shuffle tx with 3 participants and 3 ballots generated..

FEE: 0.3 MARS

180ff24e1243b2cad4387b49153517e2b6636b79b2edfe7db77fe4ca357f2dc3

MKuT7F6UHSGvfthavvdVV6rrDxUp4puZec	0.1 MARS	›	Embedded Data

One of the citizen's votes with embedded data for 0.1 MARS

scriptSig
3045022100b1da7a544bb63cd62c57e47dbaf1c9dc8b8afdd01796f37...
031a629015fa8d2e23e8cb83e4142efe10965b99a2757ac70929b394...

Type nulldata
scriptPubKey
OP_RETURN 5052595f516d587647334c466956376e6237656656416975335369694a...

PRY
IPFS Link

The embedded data contains "PRY" (Proposal YES) vote and a reference to the IPFS link that specifies the proposal voted on.

Included in Block cbce3fb7cf6eb82299cda2f87a9c7fb283b75d63d3b53b11b620a359806db7f0

rapidtables.com/convert/number/hex-to-ascii.html

Hex to ASCII Text String Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button (e.g. 45 78 61 6d 70 6C 65 21):

From: Hexadecimal
To: Text

Paste hex numbers or drop file

```
5052595f516d587647334c466956376e6237656656416975335369694
a4e723336464d7347646f323276386d336a75567533
```

Character encoding: ASCII

```
PRY_QmXvG3LFiV7nb7efVAiu3SiiJNr36FMsGdo22v8m3juVu3
```

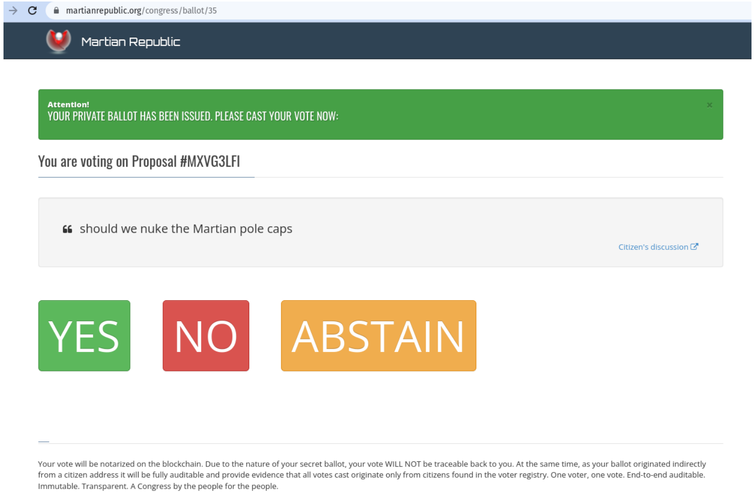
Figure 16: *The recorded ballot-shuffle and one of the citizen's vote transactions with its OP_RETURN code containing a hex encoded string with the vote and proposal reference.*

- PRY_[IPFS PROPOSAL LINK] for a "yay" vote
- PRN_[IPFS PROPOSAL LINK] for a "nay" vote
- PRA_[IPFS PROPOSAL LINK] for an abstained vote

6.6 Voting screen

Once citizens have received a valid ballot for a particular bill, they can "cast their vote" by clicking "Yes" "No" or "Abstain". The vote will utilize the new ballot balance available and spend it completely.

As the vote is merged into a data-embedded transaction on the blockchain it ties this new ballot address to the proposal/bill in question. After the vote was confirmed on the blockchain (by



Attention!
YOUR PRIVATE BALLOT HAS BEEN ISSUED. PLEASE CAST YOUR VOTE NOW:

You are voting on Proposal #MXVG3LFI

should we nuke the Martian pole caps

Your vote will be notarized on the blockchain. Due to the nature of your secret ballot, your vote WILL NOT be traceable back to you. At the same time, as your ballot originated indirectly from a citizen address it will be fully auditable and provide evidence that all votes cast originate only from citizens found in the voter registry. One voter, one vote. End-to-end auditable. Immutable. Transparent. A Congress by the people for the people.

Figure 17: *The secret ballot received, a citizen is ready to cast their vote*

a newly mined block that contains this transaction), any participant can easily check that all votes received for a particular bill were...

- ...cast only by citizens
- ...can't be traced back to any particular citizen
- ...did not depend on someone's stake but rather a majority of citizens
- ...yet are unmistakably derived from a pool of citizens via several ballot-shuffle transactions
- ...have immutable entries for the various votes anchored onto the Marscoin blockchain
- ...and in their summary make the bill's adoption or rejection inherently auditable.

Bills that pass will enter the corpus of new "laws" agreed upon by the community. A special case of "law" is a code change that was agreed upon. In which case after a server reboot, the system will pull the latest patched version of the project and attempt a restart onto the newest code and rule-set. If the launch fails, it will revert to the previous known setup. As the codebase itself is hashed, all participants can verify which version of the Constitution is currently live and active.

7 Further Integrations and Outlook

To give an outlook on the wide variety of tools that can be built around this governance system we present a few examples below. These projects have been suggested by participants of the Mars Society's Analog Desert Research Station in Utah and team / innovative researchers who needed a blockchain integration and decision making and funding process. The Martian Republic by providing the foundation becomes a useful platform to offer these tools.

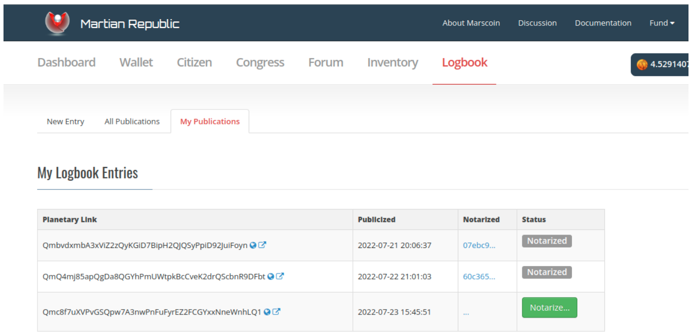
7.1 Martian Inventory

Using on-chain tracking of resources produced and allocated. This Inventory tool includes an API for systems to feed their production results into a Merkle-tree-based timestamping server for transparent inventory tracking.

Hosting this tool inside the Martian Republic allows the governance features and individual wallets interact with a stream of IoT data.

7.2 Martian LogBook

The Martian "LogBook" is essentially an online drive with Markdown editor and file upload features. This minimalistic proof-of-concept publishing platform is designed to work as a (scientific) logbook. Any publication can be notarized on-chain for recording individual and scientific data in a public format by creating an immutable record. The files and texts uploaded are distributed via IPFS on a "planetary" scale into our IPFS mesh network and made discoverable using the Marscoin blockchain. For example a version of this very paper was uploaded and timestamped and digitally notarized using the Martian Logbook. It can be retrieved via its IPFS link[40] which is embedded in an official immutable record[41] that acts as a notarized copy as referenced by the Marscoin blockchain.



My Logbook Entries

Planetary Link	Publicized	Notarized	Status
QmbvdxmbA3xViZ2zQyKGiD7BipH2QJQSyPpiD92JuiFoyn	2022-07-21 20:06:37	07ebc9...	Notarized
QmQ4mj85apQgDa8QGYhPmUWtpkBcCveK2drQScbnR9DFbt	2022-07-22 21:01:03	60c365...	Notarized
Qmc8f7uXVPvGSQpw7A3nwPnFuFyrEZ2FCGYxxNneWnhLQ1	2022-07-23 15:45:51	...	Notarize...

Figure 18: *Similar to a public online drive the Logbook features mesh network publications, albeit notarizable via immutable ledger technology*

7.3 Martian Land Registry

The Martian Land Registry is an on-chain registry of land ownership rights. Using the blockchain for notarization and timelocking of funds, the Martian land registry allows users to pre-subscribe

[40] Retrievable from `https://ipfs.marscoin.org/ipfs/QmQ4mj85apQgDa8QGYhPmUWtpkBcCveK2drQScbnR9DFbt`

[41] Recorded in block 1776110 with transaction `https://explore1.marscoin.org/tx/60c36531a7097b2ddfd0247649d6dd71b4305e8c9bcc6db27735e4f83f413fdb`

to plots of land that the public offers up for sale. The governance of land rights is thus under control of the Martian Congress - the citizenry as sovereign, allowing the public to decide the best use, distribution and protection of individual property rights.

While this is still an area of ongoing research a recent proposal takes advantage of timelocking features of the Marscoin blockchain: A citizen (still on Earth) could lay claim on a plot of land, paid for based on rules set forth by the Martian Republic as it operates on Earth. The rules could stipulate that once the Martian Republic software and Marscoin blockchain has been successfully transplanted to Mars, a citizen has a certain amount of years to claim physical possession of the land upon their own arrival. Every year the timelock expires and the citizen has to re-lock their funds to keep the claim alive.

This staking of Marscoin onto an address registered with a particular property stops when the citizen verifies his arrival on Mars via the blockchain, thus triggering his claim to become permanent. Citizens would also have the option to sell ownership to a plot of land by letting others buy ownership of a registered timelocked address. The owner could for instance forward a "token amount" to the new owner who then locks up his pledge. The Martian Republic tracks these changes and reflects them publicly. Marscoin addresses and transactions are thus used to indicate ownership. The IPFS network can be employed to showcase metadata related to the plot of land.

In a further iteration of this idea, land claims are only available to citizens who do research on the land they intend to claim. The more detailed research they do (analyzing NASA photographs of the terrain, creating a detailed study of the land they intend to purchase) the higher the likelihood of the Martian Republic citizenry to support their claim and back it up (via a form of "endorsement").

We hope that many more ideas such as the Martian Land Registry will arise and be added to this growing ecosystem. By employing similar rule-sets and combinations of on-chain notarization and IPFS data storage they are designed to involve the participation of the public in a transparent and efficient manner. It is the use of blockchain technology in a trustless, transparent and streamlined process that goes beyond commercial activity and touches a wide array of futuristic self-governance structures.

8 Acknowledgements

We would like to thank all space and cryptocurrency enthusiasts and future Martians who discussed ideas and concepts with us that led to the development of the "Martian Republic". Special thanks go to the friends and members of the Mars Society - in particular Dr. Zubrin for his relentless trailblazing efforts, the Mars One enthusiasts who gave so much of their time and efforts to bring the idea of a permanent human presence on Mars into global consciousness, SpaceX and its incredible team working day and night on making humanity multi-planetary and a physical reality. Appreciation to all Marscoin HODLers and fans that supported the Marscoin blockchain over the years and the developer community behind its blockchain and Earth's blockchain, Bitcoin.

References

[1] Wikimedia Foundation. (2022, June 2). Direct democracy. Wikipedia. Retrieved June 28, 2022, from `https://en.wikipedia.org/wiki/Direct_democracy`

[2] Kurland, P. B. (1987). The founders' constitution. Univ. of Chicago Pr.

[3] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[4] "Congress." Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/congress. Accessed 27 Jun. 2022.

[5] Grush, L. (2016, June 2). Elon Musk thinks the best government for Mars is a direct democracy. The Verge. Retrieved July 11, 2022, from https://www.theverge.com/2016/6/2/11837590/elon-musk-mars-government-direct-democracy-law-code-conference

[6] Exploring sybil and double-spending risks in Blockchain Systems. IEEE Xplore. (n.d.). Retrieved June 28, 2022, from https://ieeexplore.ieee.org/document/9435780

[7] Ruffing, T., Moreno-Sanchez, P., Kate, A. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In: Kutyłowski, M., Vaidya, J. (eds) Computer Security - ESORICS 2014. ESORICS 2014. Lecture Notes in Computer Science, vol 8713. Springer, Cham. https://doi.org/10.1007/978-3-319-11212-1_20 SpringerLink. Retrieved June 29, 2022, from https://link.springer.com/chapter/10.1007/978-3-319-11212-1_20, https://bitcointalk.org/index.php?topic=567625

[8] Bitcoinjs. (n.d.). Bitcoinjs/bitcoinjs-lib: A javascript Bitcoin Library for node.js and browsers. GitHub. Retrieved June 28, 2022, from https://github.com/bitcoinjs/bitcoinjs-lib

[9] Seed phrase. Seed phrase - Bitcoin Wiki. (n.d.). Retrieved July 25, 2022, from https://en.bitcoin.it/wiki/Seed_phrase

[10] Kosseff, J. (2022, March 16). How facebook's real-name policy changed Social Media Forever. Protocol. Retrieved July 8, 2022, from https://www.protocol.com/policy/anonymity-real-names-jeff-kosseff

[11] REPORT Barring Foreigners from Participating in Referenda Elections Dec 29. (n.d.). Election integrity. The Heritage Foundation. Retrieved June 28, 2022, from https://www.heritage.org/election-integrity and https://www.heritage.org/voterfraud

[12] Mitchell, A., Jurkowitz, M., Oliphant, J. B., Shearer, E. (2020, October 8). Political divides, conspiracy theories and divergent news sources heading into 2020 election. Pew Research Center's Journalism Project. Retrieved June 28, 2022, from https://www.pewresearch.org/journalism/2020/09/16/political-divides-conspiracy-theories-and-divergent-news-sources-heading-into-2020-election/

[13] JSON data structures. https://www.w3schools.com/whatis/whatis_json.asp

[14] Andrew Asmakov, Solana Lending DAO Overturns Vote to Take Over At-Risk 'Whale' Wallet. https://decrypt.co/103330/solana-lending-dao-overturns-vote-to-take-over-at-risk-whale-wallet

[15] Team, T. B. P. (2022, June 1). Non-custodial wallets vs custodial wallets - what's the difference?: BitPay. The BitPay Blog. Retrieved June 28, 2022, from https://bitpay.com/blog/non-custodial-wallets-vs-custodial-wallets/

[16] Schiff, I. A. (1985). How an economy grows and why it doesn't. Freedom Books. https://uplib.fr/w/images/9/9d/Schiff_how-an-economy-grows.pdf

[17] Bitcoin. (2022, January 3). Bips/BIP-0032.mediawiki at master · bitcoin/bips. GitHub. Retrieved June 28, 2022, from https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[18] Lopin, L., Burk, J., Puaschunder, P. (n.d.). Marscoin trustless-ledger technology implications for a Martian society. Retrieved July 8, 2022, from https://www.marscoin.org/whitepaper

[19] Wood, G. S. (2011). Empire of liberty: A history of the early republic, 1789-1815. Oxford University Press.

[20] Koonin, E. V., Wolf, Y. I., Katsnelson, M. I. (2017). Inevitability of the emergence and persistence of genetic parasites caused by evolutionary instability of parasite-free states. Biology Direct, 12(1). https://doi.org/10.1186/s13062-017-0202-5

[21] Baur, D.G., Dimpfl, T. The volatility of Bitcoin and its role as a medium of exchange and a store of value. Empir Econ 61, 2663–2683 (2021). https://doi.org/10.1007/s00181-020-01990-5

[22] Thomas Paine (2016). "THOMAS PAINE Ultimate Collection: Political Works, Philosophical Writings, Speeches, Letters & Biography (Including Common Sense, The Rights of Man & The Age of Reason): The American Crisis, The Constitution of 1795, Declaration of Rights, Agrarian Justice, The Republican Proclamation, Anti-Monarchal Essay, Letters to Thomas Jefferson and George Washington. . . ", p.724, e-artnow