A Sneak Peek at User Issued Assets & Security Tokens in Cardano

emurgo.io/en/blog/user-issued-assets-security-tokens-in-cardano

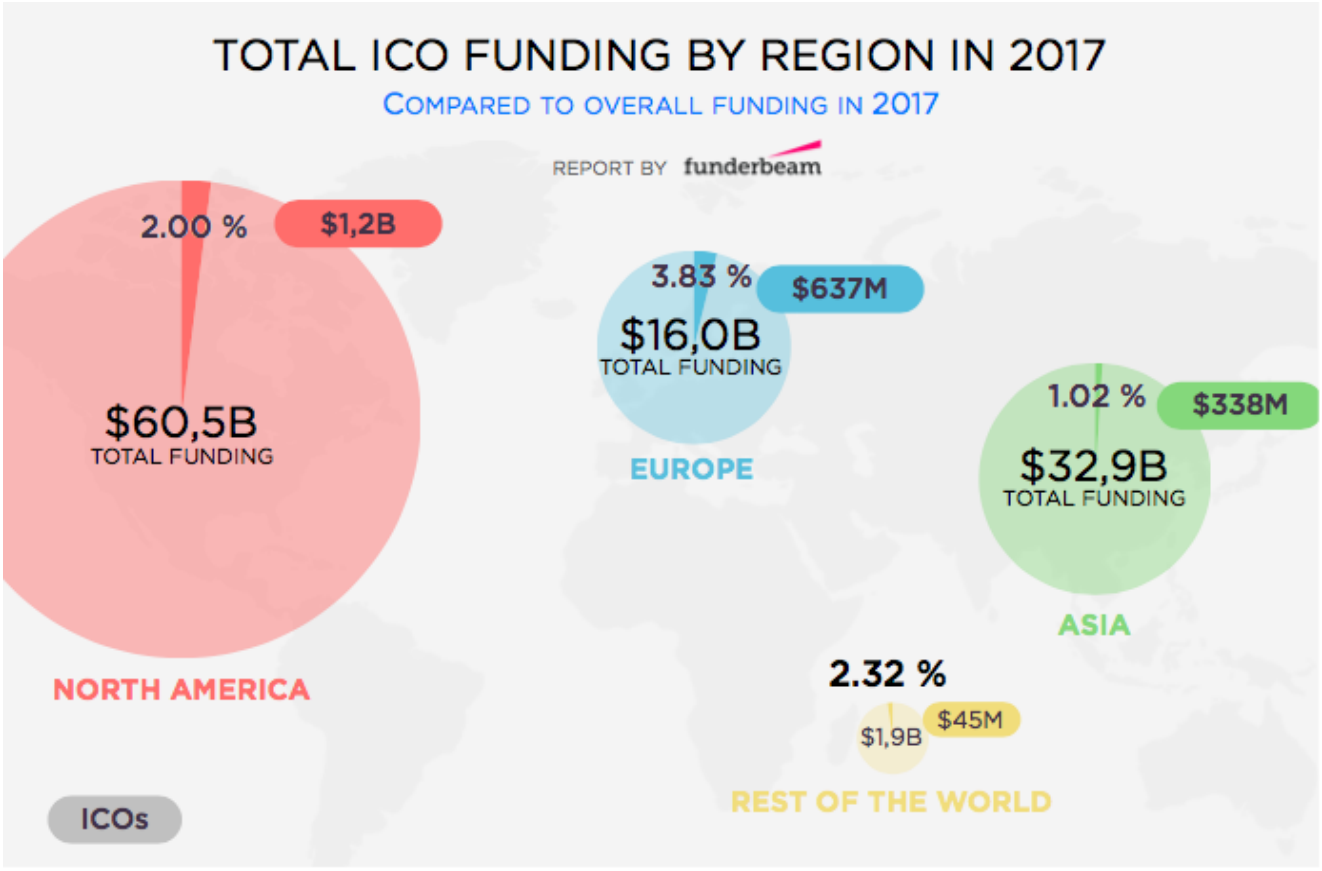
EMURGO, as the official and commercial venture arm of Cardano — the first third generation blockchain to evolve out of a research-driven approach — offers customers a complete start-to-finish advisory solution when it comes to understanding the necessary regulations their companies and security tokens must adhere to, as well as in understanding how to implement their offerings.

If you have been actively following the cryptocurrency space then you are likely already familiar with Initial Coin Offerings (ICOs) and have probably even participated in one, or more, yourself. These are basically an unregulated way for a company, or project, to raise investor funds. There were so many scams associated with ICOs in 2016 and 2017 that the SEC has identified a new category of securities for companies seeking regulated fundraising in the cryptocurrency space: ***security tokens***. Unlike ICOs, security tokens have stringent rules about who can purchase, and trade them, and how they can be advertised.

The SEC is doing its best to navigate the new blockchain space that has emerged, even as it proves to be a challenge, given a variety of political pressures and the likelihood that they are still learning how the underlying technology actually works. For example, Distributed Autonomous Organizations have thrown a bit of a wrench in their traditional definitions of securities.

A 2017 investigation of Ethereum's DAO clearly states that, "the Commission has determined that DAO Tokens are securities under the Securities Act of 1933." Then, in June of 2018, William Hinman, the SEC's Division of Corporate Finance director came out and claimed that Ethereum was not a security. And although SEC chairman Jay Clayton said that, "I believe that every ICO I have seen is a security," he had decided to agree "with Director Hinman's explanation of how a digital asset transaction may no longer represent an investment contract." This proved to be confusing for many people. Clayton humbly, and tacitly, admitted that the SEC could use more employees who are capable of understanding the technologies they are assessing.

A security is "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party." In other words, if an investment contract passes the famous Howey test, it is considered a security. However, some blockchain tokens function as both utilities and securities; and their use cases can change over time. So, while real world implementations may blur stringent categories into a spectrum of use cases, digital security tokens are the SEC's attempt to bring compliance into the blockchain and ICO space.



Source: Funderbeam

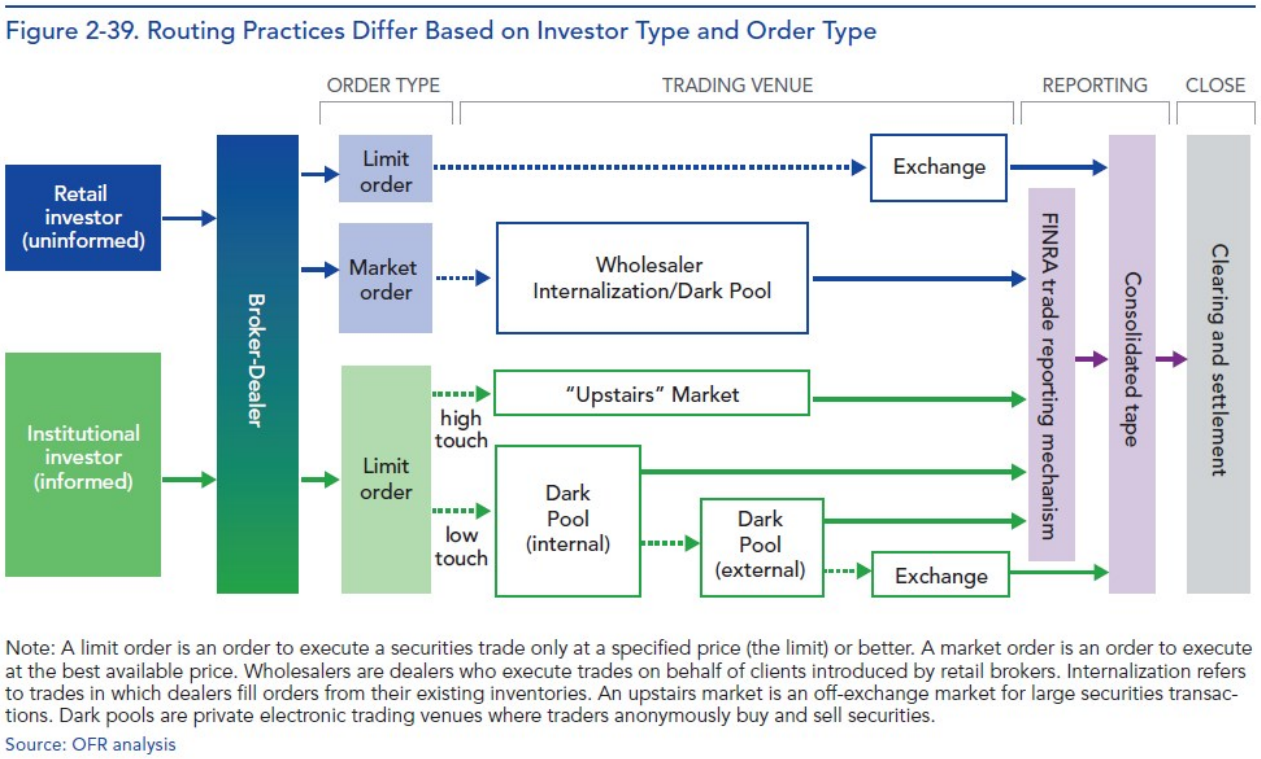
However, a Security Token Offering (STO) under Regulation D requires accredited investors to wait a minimum of one year before selling their tokens; on top of that, the counterparties for those trades must also be accredited investors. Additionally, exchanges that want to list compliant tokens need to have a special license. Barriers to entry mean that retail investors will not be able to participate in Regulation D offerings. Although this is unfortunate for some, Security Token Offerings will definitely change the cryptocurrency landscape and offer legitimacy in terms of regulation; they will also offer tremendous expansion in terms of adoption for Cardano.

Charles Hoskinson said in a recent CoinDesk interview that, "There's a tremendous desire for STOs; you have tons of illiquid assets all around the world — trillions and trillions of dollars of real estate, [and] small business, in jurisdictions like Mongolia or Ethiopia that are incredibly investible because they're led by great entrepreneurs, the economies are growing at ten percent per year, they have wonderful fundamentals from cash flow to business relationships — hundreds of millions of customers — but they haven't been able to get access to the global financial markets because of regulatory barriers as well as just bad infrastructure in those jurisdictions. So, in the pursuit of securitizing these trillions of dollars, it's creating a definite strong demand to change the regulations, change the underlying

infrastructure, and it gives us a great opportunity to build something that can be part of that conversation." There are a tremendous number of illiquid assets that traditional "emerging market" investing does not cover.

Security tokens must be Regulation D, Regulation A+, Regulation S, or Regulation CF compliant. These securities will be traded on traditional ATS exchanges (Alternative Trading Systems). Most of these systems are registered as broker-dealers and not exchanges. Interestingly, these are essentially exchanges that are semi-regulated by FINRA, exempt from the rules of a national exchange. These ATSs accounted for $16.3 trillion worth of trade way back in the second quarter of 2015. That represented "15.4% of the total dollar volume in NMS [National Market System] stocks" according to the SEC's *Regulation of NMS Stock Alternative Trading Systems* document.

The document also says that, "the Commission is concerned that the lack of operational transparency around ATSs limits market participants' ability to adequately discern **how their orders interact, match, and execute** on ATSs and to find the optimal market or markets for their orders" (emphasis mine). In other words, the ATSs are not without their own issues; and STOs will introduce a new layer of complexity in terms of how trading is allowed to happen.



Source: Office of Financial Research

It remains to be seen how exactly legacy brokers/ATSs will compete with regulatory compliant exchanges who offer their customers sophisticated, multi-pair, trading platforms and the ability to move their funds to secure (i.e., off-exchange) storage mediums. Ideally,

they will offer the same features to users. Liquidity, control over one's funds, and the ability to effortlessly move national currencies in and out of exchanges (without being arbitrarily held hostage) will prove to be valuable selling points.

Likely, we will see more global regulatory guidelines concerning STOs as the Financial Action Task Force (FATF) has already called for. As stated above, applicable regulations for STOs fall into four separate categories:

Regulation D

The SEC website states that, "Companies that comply with the requirements of Regulation D ***do not have to register their offering of securities with the SEC***, but they must file what's known as a "Form D"...[it] is a brief notice that includes the names and addresses of the company's promoters, executive officers and directors, and some details about the offering, but contains little other information about the company" (emphasis mine). Furthermore, the party offering the security tokens must solicit offerings from investors in compliance with Section 506C of Regulation D. Retail investors will not be able to participate and tokens are locked for a period of one year before investors are able to trade them.

Regulation A+

Enables a STO creator to offer an SEC-approved security token to non-accredited investors via a general solicitation for an investment totaling up to $50 million.

Regulation S

Occurs when a STO is launched in a country other than the US, and thus, is not subjected to the registration requirements of Section 5 of the Securities Act of 1933. Regulation S is composed of Rules 901 - 905; detailed information about this regulation can be found in the above link.

Regulation CF (Crowdfunding)

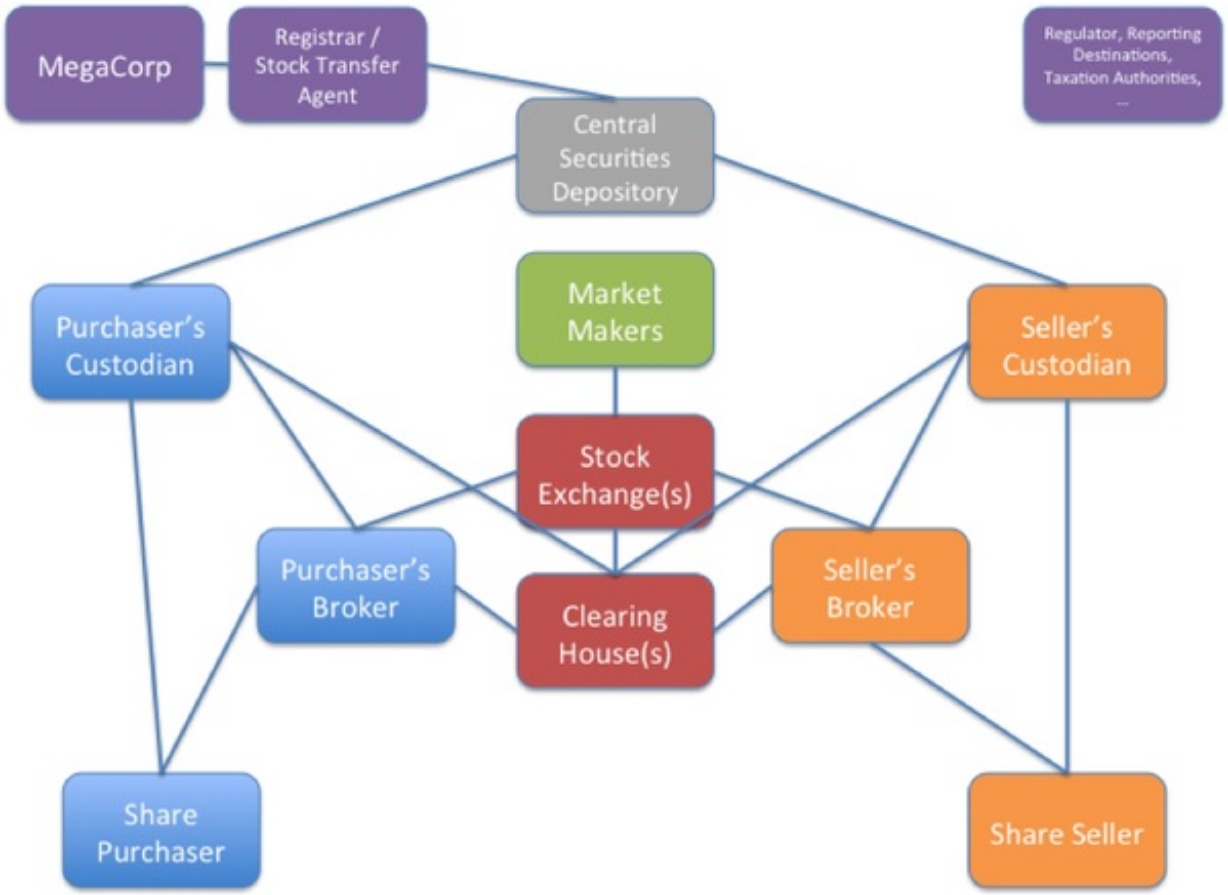
Both accredited and retail investors can participate. The offering is only able to raise $1,070,000, however. Like with Regulation D, tokens in this category are also locked for a period of one year before investors are able to trade them. Because this category allows for such little fundraising it is unlikely to see much use.

GET UPDATES THE SECOND THEY'RE PUBLISHED!
SUBSCRIBE TO OUR RSS FEED!
HTTPS://EMURGOIO-GHOST-BLOG.HEROKUAPP.COM/RSS/

Not to miss any updates from EMURGO ! Subscribe to our Blogs' RSS Feed: https://emurgoio-ghost-blog.herokuapp.com/rss/

Security tokens will allow for greater regulatory legitimization, and integration, of blockchain technologies within traditional finance and banking systems; they represent either complete, or partial, ownership of an underlying asset. However, opening up new illiquid assets and cross-border markets to investors are only a couple of the benefits that security tokens will provide; along with a greater adoption of blockchain technology, they will also help to transform the current equity clearing, and settlement, system, which is best described as a disaster waiting to happen. For example, atomic swaps and smart contracts will eliminate the need for a clearing house to act as a central counterparty during a post-trade process. Additionally, you will no longer need a registrar (UK) or share transfer agent (US) to keep track of shareholder lists or dividends. So, from a business perspective, significant costs can be cut.

In order to provide some background, Richard Gendal Brown gives us an explanation of how shares move around the securities settlement system in a 2014 blog post, which serves as highly informative reading. Below is an image illustrating how a central securities depository acts as the "custodian to the custodians;" i.e., it is an ultimate trusted third party, that no one really talks about, but who can update their master record of share ownership and eliminate the need to pass around paper, or electronic, share certificates. The efficiency of this concept is excellent; however, the concept is not secure or immutable; imagine what would happen to the economy if their systems were compromised.



Source: Brown, Richard:

"A simple explanation of how shares move around the securities settlement system," 2014.

Brown's aforementioned work was recently referenced by speaker Bruce Fenton who gave a talk at the IOHK Summit 2019; he described how the Depository Trust & Clearing Corporation (DTCC), which clears over $1.6 quadrillion in trades each year, operates on legacy, piecemeal type, third-party-trusted technology. The DTCC is currently working with IBM, Axoni, and R3 to create an open source, private blockchain, to attempt to fix the equity clearing, and settlement, nightmare system that currently exists.

However, the issue with a private chain is that, as an end user, you don't actually, technically, own your securities; their solution will be distributed, but it is not truly decentralized, nor is it a completely secure solution, as member organizations can still collude to change the chain. A private blockchain is traditionally referred to as a "permissioned blockchain."

In this context, a corporation who runs a central securities depository will "own your securities for you" (as they do now) in a way that keeps track of things in a significantly more organized, and secure, fashion than the existing system; market participants who do not trust each other will be able to interact effectively. That is a big step in the right direction. Cardano (and its partner projects) aims to be a bridge that allows users to interact with

those permissioned blockchains. The security needed to do that is both Enterprise and government grade. Private chains will be able to use Cardano to anchor transaction settlement finality with the absolute guarantee that they will never be rolled back past 2,160 slots.

Bitcoin has introduced an entirely new financial system based on a model of Unspent Transaction Outputs, hash mining, and public/private key cryptography — effectively creating an immutable global consensus. However, Bitcoin only offers rudimentary support for User Issued Assets, which are called "colored coins." Cardano looks to extend this model to support formally verified smart contracts, sidechains, Proof of Stake consensus, support for account based transactions, User Issued Assets, and regulatory compliant security tokens. These changes represent large steps forward in terms of the evolution of cryptocurrency technology. Cardano will offer a way of tracking assets through "mixed tokens" on Plutus and through interoperability with regulatory compliant tokens via "special purpose hybrid blockchains."

The *Multi-Currency on the UTxO Ledger* document examines a number of possible implementations for creating user issued currencies. Supported currencies will need to be: fungible tokens, non-fungible tokens, and mixed tokens. User Issued Assets, i.e., currencies, will be available through the Extended UTxO model on Plutus. In order to really clearly understand how the Multi-Currency / User Issued Assets system works on Cardano you need to first understand how the Extended UTxO model works. As a reader, it is important to note that this model, and its official specification, is still being developed, as of May 2019. This model extends the traditional UTxO/Bitcoin style transactions through three new scripts:

1. A validator script. This is essentially the core code behind a Plutus smart contract.

2. A redeemer script. It allows a user to collect, i.e., unlock funds.

3. A data script. The data script allows you to pass values, parameters, and "data" to the validator script.

A validator script takes a data script and a redeemer script *as parameters*, and evaluates them. If the redeemer script returns *success* then the currency is sent as indicated by the redeemer script. Traditional, imperative, programmers may not be used to the concept of a script taking another script as a parameter and then evaluating that script. Unspent transaction outputs are locked by validator scripts and inputs are unlocked with redeemer scripts. Each script, along with its hash, is stored on the blockchain and is immutable. These scripts allow a higher level of flexibility when it comes to managing how money is spent on the blockchain.

These Plutus scripts will also allow any user to forge, and issue, their own tokens. The Multi Currency document provides a provisional example of a User Issued Currency with a monetary policy using a state machine and the (state, action) tuple to pass data between steps. The document outlines 5 example steps to create a currency:

1. Select a UTXO to start.

2. Define the validator script hash of the currency (hCur) and reserve (hRes).

3. Produce two pay-to-script outputs that create an initial state transaction.

4. Forge 10,000 coins.

5. Distribute the currency and change the total Circulating amount value.

Steps 1-4 are only needed once, during the initial setup. Step 5 is needed to issue the currency. Readers should be aware that, as IOHK developer Michael Peyton says, the Multi-Currency system is still "under design" / development and this should be taken only as a provisional preview of what is possible. More will likely be known when the Extended UTxO specification is completed.

The reason that Cardano has initially considered implementing a Multi-Currency system using Plutus, and the Settlement Layer, is that having a separate side chain, or UTxO set, for each currency would likely be too impractical memory/space wise. Furthermore, having a registry of tokens that can only grow in size is also potentially problematic. In contrast to the aforementioned, initial, Plutus design, "the Polymath ST-20 standard embeds regulatory requirements into the tokens themselves, restricting trading to verified participants." Exactly how Polymesh will interoperate with Cardano is still a question that has yet to be answered. The Polymath blog says that it is time to "rewrite the foundation" with an "infrastructure overhaul." Charles Hoskinson provides some clarification in his video on interoperability with other projects.

Cardano is examining a number of different options for User Issued Assets. The Plutus implementation will allow a broad spectrum of use cases and freedom for users to create their own utility tokens, while Cardano's future interoperability standards, likely supporting Polymesh, will accommodate institutional actors who need legally compliant securities. Both of these potential implementations underscore the deeper concept of ownership, and the move to a model where you will actually own your securities from a technical perspective.

Real, structural, ownership is not a concept that most people take into consideration in their daily lives. For example, if you refuse to pay property taxes, and the government takes away your home, do you really own it? Or are you merely a glorified renter? If your bank loans

90% of your deposits to other institutions, and individuals, and credits you with an IOU, do you really own your deposits/currency? If your savings are debased through massive inflation then isn't that technically theft?

These are not merely trivial questions, but core concepts defining what constitutes your rights. A new concept has started to flourish that can be summed up quite simply: only sufficiently advanced cryptography, and mathematics, can protect your finances, identity, and personal rights.

A deeper understanding would suggest that the technical architecture and the governance systems of a society are one in the same; it is only now becoming common knowledge that you can't separate them. One might surmise that is why our current congress is filled with lawyers instead of engineers; laws can be, and are, selectively enforced, while technological standards, and protocols, are an underlying bedrock that functions absolutely.

The aforementioned new understanding concerning cryptography is partly why so many developers are now interested in financial systems, prediction markets, supply chains, identity ownership, asset management, and the blockchain. If you can relax for a moment and take a step back from all the price charts you can begin to contemplate the incredible historical significance that projects like Bitcoin, Ethereum, and Cardano represent.

Is a Security Token Offering right for your company? Reach out to EMURGO and let us help you with our STO advisory services today.

About EMURGO

EMURGO drives the adoption of Cardano and adds value to ADA holders by building, investing in, and advising projects or organizations that adopt Cardano's decentralized blockchain ecosystem. EMURGO leverages its expertise in blockchain R&D as well as its global network of related blockchain and industry partners to support ventures globally.

EMURGO is the official commercial and venture arm of the Cardano project, registered in Tokyo, Japan since June 2017 and in Singapore since May 2018. EMURGO is uniquely affiliated and works closely with IOHK to grow Cardano's ecosystem globally and promote the adoption of the Cardano blockchain. To learn more about the project, visit the EMURGO website.

|| **Click here to subscribe to the EMURGO Newsletter** ||

Follow EMURGO on Social Media

- Official Homepage: emurgo.io
- Twitter (English): @emurgo_io
- Twitter (Japanese): @Emurgo_Japan
- Youtube: EMURGO

- Telegram: EMURGO Announcements
- Facebook: @emurgo.io
- Instagram: @emurgo_io
- LinkedIn: @emurgo_io

About Yoroi Wallet

- Yoroi Twitter: @YoroiWallet
- Yoroi Homepage: https://yoroi-wallet.com/

About Cardano

- Cardano Forum: https://forum.cardano.org/
- Cardano Telegram: https://t.me/CardanoGeneral
- Cardano Reddit: