Analyst: Mrinalini Bhutoria (Ria) (@riabhutoria)

Updated: 9 August 2018

Cardano (ADA)

Price
$0.114

Avg. Daily Traded Volume (30D)
$100m

Market Cap
$2.9b

Project Announced
September 2015

Consensus mechanism
Ouroboros (Proof of Stake)

Nodes	Transactions per second (tps)
Currently centralized	200 tps (hypothetically)

Block height	Developer Team
>15,600	>30

Telegram followers
~22,000

Source: onchainfx.com, cardanodocs.org, cardanoexplorer.com

Date: As of 08/08/18 at 05:05PM ET

Launched in 2017, Cardano is a smart contract blockchain platform being developed by IOHK (Input Output Hong Kong).

The team claims that it is the first platform backed by peer-review and scientific study. The team shares its research with academics for rigorous testing prior to implementation. It is among multiple projects aiming to build a third generation of blockchain systems. It's main goals are to create a scalable, interoperable, and sustainable blockchain ecosystem.

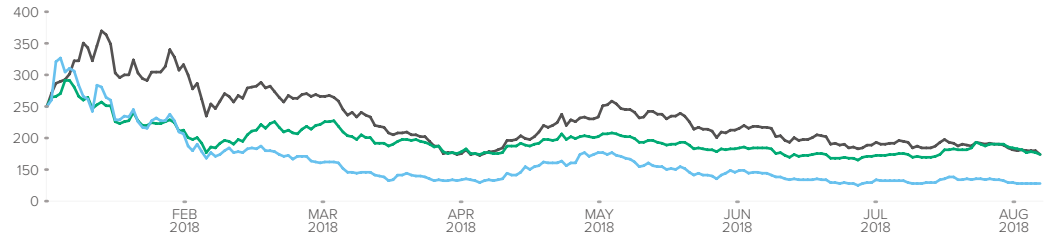
Cardano splits the protocol into two layers. The first layer is the Cardano Settlement Layer (CSL) with unit of account ADA and the second layer is the Cardano Computation Layer (CCL) for running smart contracts. The separation allows for easier upgrades and greater flexibility as the layers can progress independently of one another.

There are three entities behind Cardano. IOHK is a blockchain focused research and development company founded by Charles Hoskinson and Jeremy Wood (co-founders of Ethereum). IOHK has been contracted to work on Cardano from 2015-2020. The IOHK team includes academics and experts in engineering, network design and cryptography fields. IOHK has also partnered with universities specializing in the technologies and concepts it is using to build Cardano.

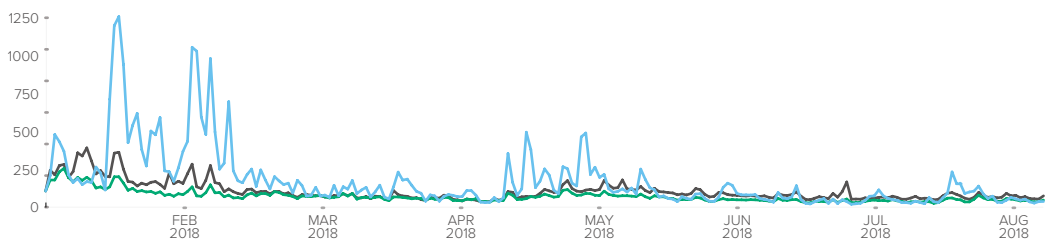
The Cardano Foundation is a Swiss-based blockchain and crypto asset standards setting body that supports research and development in Cardano, community development, and collaborating with authorities on regulatory and commercial matters. Emurgo is a Japanese venture capital firm focused on blockchain applications supporting regulatory oversight. Emurgo is likely the entity funding IOHK.

Cardano raised ~$62 million in its token sale, which took place from September 2015 to January 2017 in four presale phases with heavy KYC requirements. It was marketed to Asian buyers (who were predominantly Japanese). To date, there are 26 million ADA tokens in circulation. The maximum supply is set at 45 million.

INDEXED PRICES YTD (1/1-8/7)



INDEXED DAILY VOLUME YTD (1/1-8/7)



Additional Resources

- Website
- Whitepaper
- Twitter
- Github
- Telegram

THIRD GENERATION BLOCKCHAINS

Bitcoin is known as a "first generation" blockchain with a decentralized currency that doesn't require a trusted third party to operate. Alice can now pay Bob directly without using a central point of contact like a bank. Bitcoin also has a scripting language for transactions, but most scripts are disabled for security purposes. While it is intentionally not Turing Complete, it does provide limited flexibility to run popular scripts such as multi-sig[1].

Ethereum is considered a "second generation" blockchain because it is more programmable. Its scripting language, Solidity, is Turing Complete and thus more flexible. Ethereum decentralizes computation and allows code to exist and execute on the blockchain. However, Ethereum, Bitcoin and other early blockchains face challenges relating to governance, scalability, interoperability, security, and sustainability.

Third generation blockchains aim to take the best aspects of the first and second generations and provide infrastructure that addresses scalability, interoperability, and sustainability from the ground up, though Bitcoin and Ethereum are simultaneously building solutions to address these challenges. Cardano, specifically, plans to use include a hypothetically provably secure proof-of-stake consensus protocol (Ouroboros), delegation, parallel processing, side chains (Non-interactive Proofs of Proof of Work, or NiPoPoW), RINA (recursive internetwork architecture), partitioning, a Treasury system, and more. Not all of these tools are unique to Cardano.

ROADMAP

Cardano is being developed in multiple stages, starting with Byron (the bootstrap era), followed by Shelley (the decentralization era), Goguen (the smart contract era), Basho, and Voltaire. The Cardano token, ADA, is named after Ada Lovelace, who was a 19th century mathematician and is known as the first programmer. She was daughter of Lord Byron, a British poet, after whom the first phase is named. Goguen is named after Joseph Goguen, a computer scientist known for software engineering, formal specification, and algebraic semantics among other things. Basho is named after Japanese haiku master, Matsuo Basho. The Voltaire phase is named after French enlightenment writer, historian, and philosopher.

Byron (Complete)

The Cardano mainnet went live on September 29, 2017, kicking off Byron. Byron is known as the bootstrap era, as stake is automatically delegated to a group of trusted nodes operated by The Cardano Foundation, IOHK, and Emurgo. While the blockchain is centralized and operated by specified nodes, the transaction fees and block rewards are burned.

Shelley (In Progress)

Shelley is the path to decentralization of staking and block production in Cardano. After Shelley is complete, Cardano no longer depend on the trusted nodes. Shelley's work streams include delegation, incentives, and networking. The team is releasing specific features as they are ready. The research phase of Shelley was completed in 2Q18. The design phase will take place from 2Q to 3Q18, and implementation will occur in by April 2019, if not by the end of 2018. The team expects the Shelley testnet for staking to arrive at the end of 3Q18.

Until Goguen (the next phase) is complete, IOHK will maintain control of proposing and implementing software updates. Voting on Cardano Improvement Proposals (CIPs) will not be decentralized until later stages as the voting system is still under construction.

Goguen (In Progress)

Goguen is the next phase following Shelley. The goal of the Goguen phase is to deliver smart contract functionality for the CCL, including a new virtual machine and programming language. Cardano aims to complete Goguen by the end of 2018. Goguen's work streams include sidechain capability, IELE virtual machine and Plutus code, among others. The testnet for the IELE virtual machine was launched on July 30, 2018.

[1] Script can be used to specify that more than one private key signature is needed for a transaction to be authorized.

Basho & Voltaire

Following the completion of Goguen, Cardano will add features and functionalities as they become available. Basho will be centered around performance improvements and Voltaire will introduce a treasury and governance system.

Stage	Implementation	Complete	In Progress
Byron	Mainnet	◉	
	Currency layer	◉	
	Ourboros (Proof of Stake)		◉
Shelley	Decentralization		◉
	Voting		◉
	Delegation		◉
	Incentives		◉

Stage	Implementation	Complete	In Progress
Goguen	Smart contract layer		◉
	KEVM		◉
	IELE VM		◉
	Plutus code		◉
Basho	KMZ Sidechains		◉
	Rina		◉
Voltaire	On Chain Governance		◉
	Treasury		◉

CONSENSUS

According to the Cardano team, Ouroboros is the first provably secure proof of stake consensus algorithm. The team claims to have mathematically proven that the protocol cannot be compromised by any known proof of stake attacks. Ouroboros was designed by IOHK scientists led by Professor Aggelos Kiayias, a top cryptographer who has shown true proof of security in Ouroboros.

In proof of stake, the likelihood of being elected as a block producer is proportional to the stake via direct ownership or delegation. In Ouroboros, a stakeholder is selected ahead of time to produce a block. With proof of work, miners use electricity to crack computationally intensive problems. Computation becomes increasingly difficult (and increasingly energy intensive) as the number of miners and power of mining equipment on the network rises.

Note: The opposite is true as well. The network assesses the speed at which blocks are created every 2016 blocks and adjusts the computation difficulty such that it takes ten minutes to produce a block. If the speed of block production is slower than expected, the difficulty level is lowered. The difficulty level and speed can decline if CPUs desert the network.

One reason the team deems Ouroboros provably secure is by proving that the protocol achieves true randomness in choosing block producers (called “slot leaders”). Proof-of-stake protocols that do not have true randomness can be unfair and vulnerable to bias. Ouroboros gets its randomness from multiparty computation (MPC). Each elector[2] independently performs “coin tossing” and shares the results with the other electors. The results are randomly generated by each elector separately, but eventually the electors agree on a final outcome. This process results in the creation of a random string and the slot leader is chosen deterministically based on the string and staked coins as a proportion of total.

The process for creating randomness consists of three phases – the commitment phase, the reveal phase, and the recovery phase. This results in a randomly generated byte string called a “seed”, which is used as the element of randomness in the “Follow the Satoshi” (FTS) protocol that Cardano uses to elect slot leaders. FTS is an algorithm that picks a coin, and when coin owned by stakeholder N is selected, N becomes a slot leader. Thus, the more coins N has, the greater N’s probability of getting selected.

SEED --->| FTS |---> ELECTED_SLOT_LEADERS

Ouroboros divides time into epochs, which are divided into slots. Currently, there are 21,600 slots per epoch and each epoch lasts five days. During each epoch, slot leaders are randomly selected for the next epoch. Participants know at time N who the slot leaders are for time N+1, and this cannot be changed. The concept of epochs is needed because the distribution of coins is dynamic (is constantly changing). Thus, the blockchain takes a snapshot of the distribution at a point in time and uses that to determine slot leaders.

[2] Electors participate in MPC to randomly select block producers for each epoch.

A slot leader is elected per slot, which lasts for 20 seconds. Multiple slot leaders cannot be allocated to the same slot but one slot leader can be selected to create more than one slot per epoch. If a slot leader misses its slot, then it cannot create a block unless it is selected again. If someone is elected, they have three options: 1) create the block, 2) do nothing, 3) delegate block production rights to another person or entity.

Cardano plans to move to Ouroboros Praos, an upgrade to Ouroboros. There are a few key differences between Ouroboros and Ouroboros Praos. Praos will not rely on MPC for randomness and will provide quantum resistant signatures. In addition, in Praos, only the slot leader will know that it is a leader in the next epoch. Currently, everyone knows the slot leaders in advance.

Delegation

Stakeholders can delegate participation to some delegates. These delegates represent the stakeholders in MPC (coin tossing), block production, and voting on CIPs. Stakeholders can assign these functions to delegates using a delegate by proxy scheme and generating a proxy signing key. Stakeholders can also revoke delegation via a revocation certificate.

Ouroboros will also implement transaction endorsing as a check to incentivize slot leaders to follow the protocol. Cardano will assign input endorsers to each slot leader. Input endorsers will be randomly chosen based on their stake. A block will only be valid if these endorsers check and sign off on the transactions a slot leader is including in a given block. The endorsers will also be compensated for performing this function and incentivize good behavior.

Transaction fees

Transaction fees are used to incentivize block production to 1) compensate slot leaders for creating blocks and 2) prevent DDoS attacks (by making it sufficiently expensive to launch an attack). The formula for determining the fees is a + b*x where ‘a’ and ‘b’ are constants and ‘x’ is the transaction size in bytes. Eventually, the team wants to create a scheme that dynamically sets a and b based on the demands at any given time. The transaction fees are collected in a virtual pool and will be distributed to slot leaders of a given epoch once the network becomes decentralized. Right now, the fees are burned.

Lastly, this protocol relies on a key assumption called the “honest majority” assumption. This assumption states that the majority of participants (50% + 1) are honest and that bad actors cannot break the safety and liveness of the blockchain (liveness is the idea that “something good eventually happens” i.e. every node reaches consensus).

GOVERNANCE

Bitcoin and Ethereum use informal, off-chain governance processes. In some instances, the lack of a formal governance process has resulted in dichotomy and messy outcomes (i.e. BTC vs BCH, ETH vs ETC). In these instances, disagreement around a proposed change has resulted in a contentious hard fork. Cardano aims to fix this by using on-chain governance such that when a change or update is proposed, it could be put up for a vote by the community. If enough stakeholders support the change, it could theoretically be implemented without hard forking the network. Other projects working on their own version of on-chain governance include Dfinity, Tezos, EOS, Qtum, etc.

Cardano also plans to use a constitution as a mechanism for dealing with protocol updates in a decentralized way, though the concept is still being researched. Until then, IOHK will determine and implement software updates. We discuss this in further detail in the *Sustainability* section.

Another issue Cardano aims to address with formal governance is how the community will fund ongoing innovation. Funds from a one-time token sale will eventually run out. When that happens, Cardano plans on implementing a treasury during the Voltaire phase funded by a portion of total transaction fees as an organized way to fund continuous improvements. The team aims to allow stakeholders to vote on what projects to fund using the treasury.

CARDANO LAYERS

Cardano Settlement Layer (CSL)

The CSL is the first layer in Cardano and is the mechanism for recording the flow of ADA tokens. CSL serves the same function as the Bitcoin blockchain (as a digital payment system) but aims to fix major design flaws as determined by the Cardano team. One of the main differences between CSL and Bitcoin is that CSL uses proof-of-stake. Cardano also has a computation layer (CCL) that is separate. The entities building Cardano decided that separating accounting of value from computation would result in significantly more flexibility when designing smart contracts.

CSL has two sets of scripting languages – Simon for moving value from wallet to wallet and Plutus (currently being developed) for interoperability (and for building smart contracts). There is not much literature on Simon except that it is a domain specific language (DSL) that uses a base set of foundational elements that can be combined to enable more complex transactions. Simon is based on a paper by Simon Peyton Jones (Composing Contracts).

Eventually CSL plans to connect to CCL and other compatible ledgers via sidechains, support multiple signature schemes starting off with elliptic curve cryptography and eventually quantum resistant signatures (developers will be able to to add support for additional schemes via soft forks), allow users to create their own assets similar to ERC-20 tokens on Ethereum, and scale by running multiple epochs in parallel. However, these aspects are still a work in progress and it is unclear if/how they will function when implemented.

Cardano Computation Layer (CCL)

The CCL layer is the smart contract layer that Cardano will develop during Goguen. The intention is to provide a smart contract platform that can guarantee that smart contracts and dApps execute as intended without vulnerabilities. Two mechanisms Cardano is using is a new formally specified virtual machine and a new formally specified programming language.

Virtual Machines

Cardano plans to offer two VMs, KEVM and IELE, developed by Runtime Verification (RV)[3]. KEVM is the Ethereum virtual machine, or EVM, specified in the K framework. The K framework was developed by RV and Professor Grigore Rosu's Formal Systems Laboratory at the University of Illinois. K allows smart contracts to undergo formal verification, which results in improved security as smart contracts can theoretically run specified without bugs. Cardano launched the KEVM testnet in May 2018 and IELE testnet in July 2018.

The IELE virtual machine was built for Cardano by RV. The team claims that IELE can support smart contracts written in any programming language that has a formal semantics in K. RV's CEO, Prof. Grigore Rosu has made the following statement about IELE: **"One of the driving forces behind the initial design of IELE was to facilitate the creation of more reliable and robust smart contracts and to prevent errors in code that can lead to large-scale hacks. IELE was designed from scratch using formal methods, following the same approach we previously used to formalize the KEVM semantics. The IELE virtual machine is generated from its formal semantics completely automatically, allowing no room for programming errors. With no gap between its formal semantics and implementation, IELE enables mathematical proofs of the accuracy and security of smart contracts. IELE smart contracts are also human readable, making them easy for businesses to adopt and use."** IELE also uses a compiler that translates Solidity code into IELE to allow Solidity developers to test the same code on IELE. The team plans to eventually roll out compilers that allow the translation of other programming languages that have specifications in K into IELE.

Programming Language

Smart contract developers will be able to build dApps and smart contracts using Solidity. In addition, Cardano has hired a team of developers to create an entirely new, high assurance language called Plutus. Plutus is a functional and human readable language, like Haskell. Unlike Haskell, Plutus has formal specification. Functional languages (as opposed to imperative languages) are more precise, limit human error, and make it easier to achieve the intended coded outcome i.e. it is easier for programmers to verify that the code is being written correctly early in the development process. The downside of developing a functional language is that

[3] RV has worked with companies that require secure, mission critical software like Boeing, NASA, and Microsoft.

there are fewer developers that have experience coding in a language like Haskell (Note: Unlike Plutus or Haskell, Solidity is an *imperative* programming language). However, the reason Cardano is developing such a language is to prevent code flaws and thus prevent unintended events (such as the DAO and the Parity wallet hack). Eventually, Cardano will also integrate support for multiple smart contract languages.

FEATURES

Scalability

Cardano breaks down scalability as it refers to crypto assets into three different aspects – throughput in transactions per second, bandwidth, and data scaling.

Throughput

Throughput refers to the number of transactions that can fit into a block within a finite period of time. A common way to measure throughput is transactions per second (tps). In order to allow for greater tps over time, Ouroboros has been designed in a future proofed and modular way. Eventually, Cardano plans to run multiple epochs in parallel and partition transactions into multiple epochs. Further, slot leaders will be able to produce blocks in multiple chains because with PoS, the cost of producing a block is low. As the number of users grows, the idea is that slot leaders will be able to maintain multiple blockchains concurrently and process transactions in parallel. Charles Hoskinson recently said Cardano was able to process 200tps in a lab environment unsharded.

Bandwidth

Transactions carry data and as you get more transactions you need more network resources. For a system to scale to millions of users, the system could require gigabytes of bandwidth per second to support all the data flowing through it. Thus, it will be impossible to scale a system where every node has to relay every piece of information. To confront this, Cardano is exploring RINA – recursive internetwork architecture. RINA is a new way of structuring heterogenous networks such that every node doesn't have to process every transaction, though there is not much additional information on the topic to date.

Data

Blockchains store information forever. As tps grows, the amount of data grows, and the size of the blockchain grows from megabytes to petabytes and beyond. This makes it difficult to scale in a peer-to-peer world where storing a copy of the entire blockchain is how the network is secured. Cardano plans to use partitioning to scale the data aspect. With partitioning, nodes don't get the entire blockchain but rather a part of the blockchain. However, Cardano wants to ensure that it has the same level of certainty about the state of the blockchain as if the nodes stored the entire blockchain.

Interoperability

Crypto assets are not seamlessly interoperable with one another or with traditional systems. Value and information cannot be easily transferred across blockchains (i.e. from Bitcoin to Ethereum) or from blockchains to traditional systems in the same way that information can be sent seamlessly from Gmail to Yahoo. Cardano is one of multiple projects working on interoperability solutions between blockchains and between blockchains and traditional systems.

Blockchain to Blockchain

As it relates to blockchain to blockchain transfers, Cardano is researching how to structure information and value traveling from one chain to another in a compressed manner such that the recipient has the ability to know with certainty that the transaction is legitimate (1 - the sender has the value, 2 - the sender has not double spent the value).

In order to facilitate blockchain interoperability, Cardano plans to use KMZ sidechains (a protocol developed by Kiayias, Miller, and Zindros) that use proofs of proof-of-work to facilitate cross-chain transactions. The idea is that KMZ sidechains will be able to compress and transfer data across chains in a secure way that prevents double spend attacks (see here for a more technical explanation of how this works). Compressing the data is necessary given that there are thousands of crypto assets in existence and each of these crypto assets' blockchains are growing in size day by day. Implementation of side chains is still in the research phase and has not been implemented.

Blockchain to Legacy

Legacy systems are more complex as they require certain components in order to be compliant with internal and external rules and regulations. These components are metadata, attribution, and compliance.

Metadata

Metadata refers to the story behind a transaction – where did you spend it, on what, to whom, etc. This information is very important in traditional financial systems as it determines the level of risk associated with a transaction. The problem with metadata in the blockchain universe is that blockchains are transparent and immutable, and attaching such sensitive data to transactions on a blockchain could result in exposing sensitive information to the wrong set of eyes. Therefore, Cardano is researching where, when, and how to put metadata on a blockchain without compromising sensitive information. Some ideas include encrypting the data or using a scheme that only allows certain people to view it.

Attribution

Attribution refers to the identity of the parties in a transaction. It is a subset of metadata, but one that Cardano deems very important so it has its own discussion. Crypto assets have the tools to store public keys and develop different webs of trust. Cardano is starting to explore how it can use tools for storing money in crypto systems and apply them to attribution (i.e. being able to share identity when sending money to an exchange).

Compliance

Compliance refers to requirements such as KYC (know your customer), AML (anti-money laundering) and ATF, or pieces of information needed to prove that a transaction is legitimate. These are requirements of all money services businesses that handle money on behalf of customers.

Cardano wants to put these components together on a voluntary and case by case basis that allows the crypto world to interact in a compliant way with legacy systems. By using cryptography, optional metadata, and trusted hardware that can allow secure ways of storing credentials and potentially even provide guarantees that sensitive data has been destroyed after a period of time.

Sustainability

The sustainability of crypto assets has two components: how to future proof the funding of growth in a blockchain system and how do we future proof a blockchain system, recognizing its dynamic nature.

Currently, the industry funds itself is by conducting ICOs, which puts a large sum of money in the developers' hands at once. However, it is inevitable that these funds will eventually run out. One way to ensure that funds are available for future protocol improvements and projects is by using a Treasury system (such as Dash's Treasury system). In such a system, some portion of newly minted ADA tokens and transaction fees (yet to be determined) are deposited into a decentralized bank account. Then, users can vote on funding ballots submitted to the system – anyone will be able to submit a ballot. If a ballot gets enough votes, the ballot will be funded some portion of funds from the Treasury. Cardano is currently researching the best way to implement a Treasury by using a liquid democracy and an incentivized treasury model. The team plans to roll out the Treasury by mid-to-end of 2018, dependent on the research.

The second component of sustainability refers to implementing a process to future proof a dynamic blockchain system. To do so, IOHK plans to implement a constitution. By treating a protocol like a constitution allows the participants to amend and change it in a slow, methodical and deliberate way. Once Cardano implements the treasury and voting system, it plans to use the same voting process to allow participants to vote on Cardano Improvement Proposals (or CIPs), with a more rigorous process for anything that would require a hard fork and an easier process for anything that requires a soft fork.

High assurance code

Cardano is using "high assurance code" to build the platform and plans to allow developers to use high assurance code to build smart contracts on the platform. High assurance code undergoes formal verification to guarantee that it doesn't fail when implemented. Industries that rely on high assurance code include aerospace, nuclear, and medical where reliability is of utmost importance. Most crypto assets to date use low

assurance code, but a system that aims to provide financial infrastructure for the foreseeable future (among other things) should have high assurance that it will not fail or be compromised.

Cardano's approach is to use reasoned arguments and mathematical proofs to create evidence that the software is actually correct before it is implemented. Developers can write proofs about whether their program meets a certain specification or not. In order to do so, developers need to use programming languages designed to help them reason about programs as mathematical proofs. For this reason, Cardano is being built using a programming language called Haskell, which is inspired by mathematics. It is also developed a programming language that developers can use to build high assurance applications called Plutus. Plutus is based on Haskell.

DAEDALUS

The Cardano team has also built a wallet for ADA called Daedalus. Users must download the wallet to use their ADA tokens. The wallet will also be used for voting and delegation. Eventually, the team plans to roll out an app store and add support for multiple crypto assets within Daedalus.

USE CASES

- GRNET, the national research and education network of Greece, is working on a pilot project with IOHK to verify student diplomas on Cardano. The reason for putting diplomas on a blockchain is that it cuts out paperwork and makes it easy to verify whether someone has a qualification or not.
- Traxia has committed to building on Cardano, but as the CCL is not yet live, it conducted its ICO on Ethereum and will transition to Cardano once the CCL is implemented.
- Cardano has formed agreement with Ethiopian government to implement blockchain solutions in the agriculture industry.
- Partnered with London-based think tank Z/Yen to explore proofs of concept and new use cases for Cardano.
- Other general use cases the team has highlighted include unbanked or underbanked, financial services, supply chain, etc.

RISKS & CHALLENGES

Work in progress.

The majority of risks and challenges stem from the fact that Cardano is still a work in progress. To date, Cardano has yet to become decentralized (as the three entities are still operating trusted nodes) and the Cardano Computation Layer (CCL), or the smart contract layer, is still under construction. The scalability, interoperability, and sustainability are still ways away and likely won't be rolled out until 2019-2020.

Ethereum dominates

Cardano claims to be a third generation blockchain because it will solve the scaling, interoperability and sustainability challenges in "older" systems like Ethereum. However, Ethereum is working on its own set of scaling and performance improvements and has a similar timeline of 2-3 years. If Cardano and Ethereum roll out scalability and performance features at the same time, Cardano will not necessarily be a more competitive platform. In addition, Ethereum has greater development activity and community support. Cardano benefits from building scaling and performance solutions into the blockchain from the ground up.

Partitioning transactions

One scaling mechanism Cardano plans to use is partitioning transactions. At the moment, there is not sufficient information to prove that this will be easy to implement. For example, it is unclear how blocks from different partitions will fit together or how double spend attacks will be prevented across partitions. However, it is still early days and it is likely that the team will answer these questions prior to rolling out the functionality.

Programming language

Initially, Cardano suggests that developers build applications using Solidity (the same programming language used by Ethereum). However, using Solidity will yield low assurance applications whether they are built on Cardano or Ethereum. In order to build high assurance applications and smart contracts, Cardano is developing a new functional language called Plutus. The problem is that there are fewer developers who already know how to code in Haskell. Even those that do will face an initial learning curve to build apps using Plutus. To help with the situation, Cardano is building a Plutus library that developers can use.

On chain voting

The purpose of on chain voting is to represent the whole community in determining the future of the platform and prevent community splits. However, the proposals will likely be technical and difficult for a general platform/token user to understand. This could result in users without a technical understanding of proposals relying on and voting in accordance with a smaller group of programmers, and this group would have power to drive key decisions.

Formal verification

What's the catch? Formal verification allows developers to test that code will run as specified when it is implemented. However, it is possible that certain properties are missed in the process and only manifest once the code is implemented. Thus, formal verification is only as good as developers' ability to create specifications.

Reliance on academics and universities

The pitfalls of incorporating academics and universities into every aspect of the blockchain design is that it slows down the development and time to market. It has resulted in a lot of research papers but very little code, as many of the research papers are currently undergoing implementation. The advantage is that every aspect of the protocol is designed and vetted by domain specific experts.

CONCLUSION

Cardano claims to be a rigorously tested platform that promises innovations in consensus, governance, smart contract security, interoperability, and sustainability. It is one of the first smart contract networks to use high assurance code to build the platform and give developers the ability to build high assurance applications. However, the platform is still centralized, the smart contract layer has yet to be implemented, and key innovations around scalability and interoperability are still in research and development phase. It is difficult to know at this time whether it poses a threat to Ethereum (and other competing projects) as the dominant permissionless smart contract platform, or whether it will be better suited for permissioned, enterprise environments where the assumptions that Cardano is built upon are more realistic.

Disclosures

Sources

cardanodocs.com/introduction/

whycardano.com/

cardanoroadmap.com/

cardanodocs.com/glossary/#paper

forum.cardano.org/t/summary-of-project-shelley-may-2018-update/12853

blog.icoalert.com/the-ethereum-challengers-ep-3-cardano-ada-26b7e82c793

medium.com/on-the-origin-of-smart-contract-platforms/on-the-origin-of-cardano-a6ce4033985c

youtube.com/watch?v=2DFYBb_zOpc

youtube.com/watch?v=_BnBmBZPvS8

youtube.com/watch?v=Ja9D0kpksxw

coincentral.com/cardano-beginner-guide/

stocksgazette.com/2018/04/12/cardano-ada-delivers-good-news-as-shelley-approaches/

medium.com/@BitcoinByte/a-blockchain-with-privacy-and-regulation-cardano-3606e1288bc2

xbt.net/blog/what-is-cardano/

reddit.com/r/cardano/comments/7z63ia/writing_smart_contracts_on_plutus/

hackernoon.com/cardano-ethereum-and-neo-killer-or-overhyped-and-overpriced-8fcd5f8abcdf

cryptobriefing.com/what-is-cardano-introduction-ada/

weusecoins.com/what-is-cardano/

medium.freecodecamp.org/what-does-it-mean-when-code-is-easy-to-reason-about-4e6f63eb386f

medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

bcfocus.com/news/cardano-ada-breaks-down-functions-of-shelley-project/18594/

medium.com/chainrock/cardano-peer-reviewed-blockchain-for-the-thrid-generation-analysis-review-8c697a619bce

steemit.com/cardamon/@dan/peer-review-of-cardano-s-ouroboros

reddit.com/r/cardano/comments/826mmv/opinions_on_shelley_release/

paymentweek.com/2018-7-30-iohk-launches-iele-virtual-machine-testnet-cardano-blockchain/

reddit.com/r/cardano/comments/77ej8i/cardano_vs_eos/