Cardano (ADA) : the first provably secure proof of stake algorithm, peer reviewed by academics

Published on December 7, 2019

Piotr Arendarski, Ph.D
Chief Economist and Head of Cryptocurrency Research at Blockchain Board of Derivatives

5 articles ✓ Following

BBOD Rating

ACCUMULATE: An opportunity to buy a medium risk cryptocurrency at a low price

Overview

Cardano is a decentralised and open source public blockchain that seeks to address the key inadequacies of existing models by utilising a scientific philosophy with its foundations built upon a peer-reviewed academic framework. Thus, the project is developed by a global team of leading academics including the former CEO and Co-Founder of Ethereum, Charles Hoskinson, who understand that in order for a blockchain to achieve real-world utility it must be simultaneously secure, flexible and scalable. Consequently, considerable thought and time went into the development of the base layer protocol, with research commencing in 2015 before the official launch date in late 2017. Such scientific rigour combined with the implementation of Haskell, an industrial grade coding language, has allowed Cardano users assurance that the underlying infrastructure is fundamentally secure akin to mission-critical systems such as aerospace and banking. Ultimately, Cardano intends to tackle the problems of scalability, interoperability, and sustainability by utilising a distinct two-layer architecture and democratic governance model.

Scalability

Perhaps the biggest issue facing blockchain protocols today is scalability. The most notable blockchains, Bitcoin and Ethereum, can currently only handle a measly 7 and 15 transactions per second (TPS) respectively. When up against established payment titans such as Visa who process 24,000 TPS, it is hard to fathom how mainstream adoption of cryptocurrency as a means of transfer will ever occur. Of course, there are blockchains such as Ripple which can handle 1,500 TPS, but such projects are accompanied by huge trade-offs, sacrificing protocol security and decentralisation for speed. There have been several attempts to solve the issue of scalability such as Bitcoin implementing the Lightning Network and Ethereum introducing Sharding. Yet ultimately, the foundations that such projects have been built upon did not have sufficient provisions for scalability from their inception. Although they may find workarounds which allow them to pick up speed over time without sacrificing security, at current, they simply aren't viable platforms for mainstream adoption.

Interoperability

As the cryptocurrency ecosystem continues to mature, although there will be dominant blockchain protocols such as Bitcoin is today there will also likely be numerous other blockchains that will need to interact with one another in a seamless manner. Moreover, blockchain platforms must have the ability to interact with traditional legacy systems where necessary. Comparably, in the traditional finance world, banks must use SWIFT, ACH and SEPA simultaneously without the end user ever needing to be concerned with what is happening behind the scenes. This is where interoperability between different blockchains comes into play. The problem lies in deciphering how blockchains which are already extremely complex in and of themselves should communicate with one another. This is no easy feat and has yet to be achieved to proof of concept by any blockchain project in the market. Yet it is essential for individuals to utilise cryptocurrencies to their fullest extent moving forwards. Without interoperability, one would have to rely on a single blockchain for all use cases. In reality, this is highly inefficient as every blockchain will have their own unique strengths and weaknesses that users should be able to combine to form a perfectly functioning network. Ultimately, interoperability needs to be achieved without the end user ever needing to be concerned they are switching blockchains in the first place.

Sustainability

Thus far, financing models in the cryptocurrency market have been barely thought through in terms of sustainability. Although firms have managed to achieve astonishing sums of money from ICOs in the 2017 bull market, the model certainly isn't sustainable in a bear market, especially as regulators continue to crack down on ICOs. Moreover, ICO funding requires the team to allocate funds in a responsible manner to ensure the long term success of a project. Although a large war chest may take you so far, how does a project continue to succeed when th

party to fund a considerable amount of their project then they can expect that investor to have a considerable say in the direction of the business. Such centralisation is exactly what blockchain technology is trying to escape and thus it is integral that governance models not only seek to provide for their users but also for the development of a projects longevity. Ultimately, Hoskinson understands that such complex blockchains are not adopted overnight and consequently funds must be in place for years if not decades of experimentation.

Solution

Scalability

After observing the failures of other blockchains ability to scale, Cardano designed a layered architecture which splits different blockchain functions into independent software stacks. By separating the platform into a series of distinct layers, the project has the flexibility to upgrade one aspect of the platform without interfering with other functions. Ultimately, this allows for simpler platform maintenance, ensuring upgrades are implemented swiftly and allowing the platform to develop at a much faster pace than competitors who have to alter the entire blockchain in order for progress to be made. For example, in the past lack of foresight by well-known industry players such Ethereum has led to contentious hard forks that have taken time and diluted network effects. Alternatively, Cardano will never have to deal with such issues, instead, any upgrades will be made by means of soft forks. The layered architecture works as follows, the first stack concentrates on settlements between parties on the blockchain utilising the Cardano's native currency ADA. This initial layer allows individuals to transact value with one another, Cardano hopes this will lead to financial inclusion for the billions of unrepresented individuals in the banking system today. The second layer focuses on smart contracts, which are the digital enforced legal agreements that are likely to underpin the future of business. Finally, Cardano will provide a platform that will run Dapps that individuals, organisations and governments may utilise. Ultimately, the Cardano project is in this space for the long-haul and although their TPS may not significantly pass competitors such as Ethereum by much at current, the way their blockchain has been designed allows for long-term scalability.

Interoperability

In order to solve the issue of interoperability between blockchains, Cardano is implementing an innovative sidechain protocol which allows value and information to be safely transferred between two independent chains with ease. Such a mechanism will initially be used in order for the internal layered architecture to transfer value and information between the settlement layer and the smart contract layer. Once this has been achieved and the project grows in user base, Cardano will strive to create bridges between their independent blockchain and other distinct chains within the ecosystem. Additionally, although the ability to integrate Cardano into traditional legacy systems is very much a w

transparency is an excellent example of just how research-driven the project is and one would be hard pushed elsewhere to find such complex ideas expressed in an easier understood format for their users. Ultimately, Cardano is making clear progress towards achieving interoperability by using a methodical approach to ensure that the concept operates perfectly internally before trying to integrate into distant blockchains in an inadequate manner. This is a testament to the scientific philosophy of Cardano and will surely serve its users well in the long run.

Sustainability

Base layer blockchain protocols need longevity in order to ensure they can compete in years to come when mass user adoption begins to occur. In order to achieve this Cardano has implemented a Proof-of-Stake (PoS) consensus mechanism named Ouroboros. One of the key attributes of this governance model is the treasury provided by transactions that occur on the Cardano blockchain. Essentially, Ouroboros has sustainability baked into its code as a 25% of the block reward for each transaction is placed into the Cardano treasury to help foster the growth of the ecosystem. This innovative use of block reward ensures the project can organically finance itself for as long as the network is functioning, the greater the project grows the more funding it will have to ensure its future. Besides, the initial funding round of 63 million USD should be plenty to keep the project up and running until user adoption can flourish. Ultimately, this mechanism avoids involving any centralised party in the project for the sake of financial necessity. This will allow Cardano to grow in the decentralised nature as initially intended, sticking true to the morals that should be upheld by all projects within the cryptocurrency ecosystem, yet are often not.

Catalysts

Longevity: Unlike many blockchain platforms which seek to become the market leader as quickly as feasibly possible, Cardano has disguised itself by introducing a more methodical approach comparable to that in scientific communities. Consequently, although such a research-driven strategy will not necessarily see the quickest implementation, Cardano is far less likely to suffer from bugs and critical failures as many other projects will likely show in time. This should provide investors assurance that the project is a safe long-term investment.

Hindsight: Since Cardano began development in 2015 and did not rush to enter the altcoin bull market in 2017 it has learnt from the mistakes of its competitors, especially concerning scalability. Such patience to provide users with an improved layered architecture that may now actually be able to scale to tackle the needs of those who are unrepresented in the financial system today shows that the project founders are certainly not in this to make money. Instead, Hoskinson and his vast distributed team of researchers appear to truly care for the needs of their users which with time will certainly build a strong and

market should not be underestimated.

Introduction of Futures contracts: BBOD, the world's major cryptocurrency derivatives exchange, has announced that it is launching ADA futures contracts with up to 25x leverage. Cardano project was selected as one of 16 most popular and promising projects with the most enthusiastic community and promising technology.

Risk Factors

Highly Saturated Market: If Cardano is to succeed as a smart contract platform for Dapps to be built on top of then it must compete against the numerous other blockchain platforms that already exist within the market today. As most are aware, the majority of Dapps are currently built on top of Ethereum, but other projects such as NEO and EOS are nurturing a small group of Dapps themselves. Despite this, It is worth noting that Cardano's smart contract platform will be compatible with Ethereum smart contracts. This enables developers to transition their code over to the platform if they believe Cardano is more suited to their needs. In the long run, this may well be the case.

Project Scale: Cardano is hugely ambitious in scale and with its research-driven approach the implementation of the project for real-world use cases is likely to take a considerable amount of time. That being said the market is certainly still in its early adopter phase and being seen to be the market leader at current is not necessarily beneficial if users do not actually adopt the technology for another decade. If Cardano can achieve all it has set out to accomplish then it will certainly be a key contender in the market when mass adoption is actually present.

Conclusion

The research-driven approach that Cardano has chosen to implement to the development of their project speaks volumes in a market that is largely diluted by cryptocurrencies which appear to only be seeking short term gains. The goals of Cardano are certainly ambitious, yet appear feasible if the same transparent methodical steps are taken to slowly improve upon the solid foundations that have been established since the inception of the project. If achieved, Cardano could present itself as an immutable means of transfer of value and information for those who are truly in need. As developers and users become more informed on their options for creating smart contracts or utilising a blockchain network for self-gain, Cardano will surely be seen as one of the most secure and sensible blockchains to take advantage of. The road to a fully functioning blockchain network is certainly long but that should not deter savvy investors or users who are in this space for the long haul. Certainly, a blockchain platform to keep on your radar as the cryptocurrency ecosystem continues to evolve.

Telegram: https://t.me/BBODCommunity

Twitter: https://twitter.com/BBODTrading

Facebook: https://www.facebook.com/BBODTrading

YouTube: https://www.youtube.com/c/BBODTV

Linkedin: https://www.linkedin.com/company/bbod

BBOD Rating Standard

BUY: A low-risk buying opportunity

ACCUMULATE: An opportunity to buy a medium risk cryptocurrency at a low price

SPEC BUY: A speculative opportunity for investors with a higher risk tolerance

HOLD: Maintain current levels of position until further research is published

SELL: Investment is associated with the potential of losing capital

Disclaimer. BBOD Research is an independent cryptocurrency research-house. The company has not received any remuneration (cryptocurrency or otherwise) in preparing this analysis. This report has been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy in respect of any financial instruments or the issuers thereof. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research under the Market Abuse Regulation (EU) No 596/2014. Reports issued by Trade the Future Holding (“BBOD Research”) or its affiliates are not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and are not recommendations to buy, sell, or hold an asset. The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date and are subject to change without notice. BBOD Research will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents. Trade the Future Holding and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research.