RESEARCH REPORT

Cardano

INTELLIGENT
TRADING

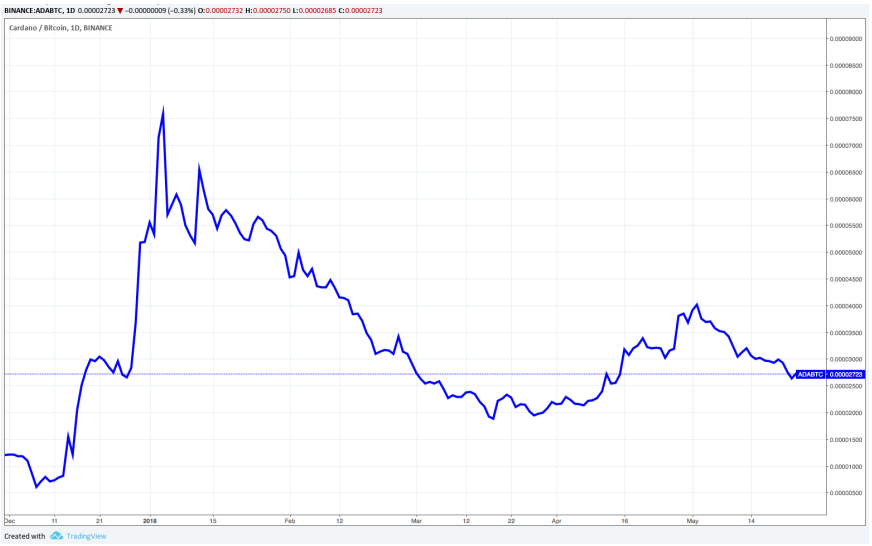
CARDANO (ADA)

Type: Platform
Date: 25-May-2018

Price: $0.21 / 0.00002723 BTC*
Market Cap: $5.4 billion
Mainly traded on: Upbit, Binance
HQ: Switzerland, Japan
First USD Price: $0.02
ICO Date: Dit Not ICO

90-day BTC Correlation: 0.42 (medium)

90-day ETH Correlation: 0.57 (medium)



Summary

The Cardano project began in 2015 with an aim to build on the strengths of Bitcoin and Ethereum and address their scalability pitfalls by introducing two protocol layers to separate accounting from computation. The project's emphasis on sound protocol design has led it to adopt a high assurance functional code while its proposals have undergone academic peer review before being implemented. The project uses proof of stake consensus protocol, called Ouroboros. Ouroboros is a unique take on a consensus protocol that is the product of a concerted effort by cryptographers from various academic institutions to improve upon existing methodologies.

Strengths

- Clear goals and extensive timeline. Vast array of information available on roadmap and proposed technologies.
- Utilizes programming language that is expressed in mathematical functions, which means the code can be vetted on a mathematical basis.
- Proposals undergo review by third party academic institutions in the field of cryptography before being implemented.
- Ouroboros is the first proof of stake to be provably secure.

Opportunities

- Cantra prepaid card supports ADA, which is accepted at 36 million locations worldwide with plans to expand even further
- For long term, ability to securely transfer metadata enables Cardano to provide borderless financial services at a fraction of legacy prices
- Projects Sp8de and Traxia to start running on Cardano platform

* as of May 25, 2018

Analysis of Cardano (ADA)

Project Analysis
- Overview
- Team

Notable Features
- Layered design
- The ADA Token
- Ouroboros proof of stake
- Soundness of protocol design

Proposed Solutions
- Technological and political scalability
- Secure transference of metadata
- Regulation without sacrificing privacy
- Interoperability with other financial systems

Project Roadmap

Roadmap Progress

Strategic Analysis
- Strengths
- Weaknesses
- Opportunities
- Threats

Technical Analysis
- Correlation with BTC
- Correlation with ETH
- Technical Forecast

Suggestions For Investment

Project Analysis

Overview

The Cardano project began in 2015 with an aim to build on the strengths of Bitcoin and Ethereum and address their scalability pitfalls by introducing two protocol layers to separate accounting from computation. The project's emphasis on sound protocol design has led it to adopt a high assurance functional code while its proposals have undergone academic peer review before being implemented. The project uses a Ouroboros proof of stake consensus protocol, the product of a concerted effort by cryptographers from various academic institutions. It also seeks to manage the political aspect of a cryptocurrency evolution by introducing formal systems of settling ideological disputes and vote on forks.

Team

The core Cardano team consists of the Switzerland-registered Cardano Foundation, which is responsible standardizing and promoting the project; the tech company IOHK, which is in charge of designing, building, and maintaining the Cardano platform and includes Ethereum co-founder Charles Hoskinson; and the Japanese-based startup investor EMURGO, which helps integrate businesses into Cardano's blockchain ecosystem.

Notable Features

Layered Design

Cardano decided to separate the accounting of value from the reasons for moving the value. The project therefore consists of the Cardano Settlement Layer (CSL) and the Cardano Computational Layer (CSL) which are connected by a new sidechain protocol called KMZ to move value between the two layers.

Released in September 2017, CSL delivers the core promise of blockchain technology as a timestamped and immutable database of facts and events. CSL provides transaction record keeping similar in function to Bitcoin but is also able to connect with CCL and move funds when conducting customized transactions that require additional programming. The protocol currently uses elliptic curve cryptography for signatures and plans to support other schemes in the future, with a particular interest in adopting schemes that are quantum computer resistant.

On the other hand, the upcoming CCL contains the context and conditions behind transactions and serves a decentralized virtual machine for running applications similar in function to Ethereum. While CCL also supports Ethereum's programming language for low assurance applications, it utilizes a new programming language called Plutus that provides strong operational semantics and high assurance of correct implementation of applications.

The ADA Token

ADA is the cryptocurrency of the Cardano blockchain that can be used to send value and serve as the native token used to run applications on the Cardano Computational Layer. In addition, holders of a qualifying amount of ADA coins will be eligible for being elected a slot leader in the Ouroboros proof of stake protocol.

Ouroboros Proof of Stake

Ouroboros proof of stake is an academically peer reviewed protocol that divides time into epochs. Delegates known as slot leaders are selected for each epoch and each slot leader is assigned a slot within the epoch to mine. Anyone who possesses a qualifying amount of ADA coins is eligible for being elected a slot leader. The selection process randomly picks a set of coins in the coin supply and the owner of those coins are selected as the slot leaders. Therefore, the more coins one possesses, the greater the likelihood that they will be holding the winning coins.

Ouroboros proof-of-stake prevents mining centralization by eliminating the need to amass large amounts of computing power to successfully mine blocks and selecting slot leaders based on a lottery system. Both the settlement (CSL) and computational (CLL) layers utilize Ouroboros proof of stake.

Soundness of Protocol Design

The project takes a slow and academic approach towards development. It is willing to undergo costly, time consuming, and tedious processes to ensure that the protocol is correctly designed. As opposed to other major cryptocurrencies, its protocols undergo extensive peer review and academic scrutiny before implementation.

In addition, Cardano utilizes a Haskell-based functional programming language which is expressed in mathematical functions. This enables the programmer to mathematically prove the soundness of the protocol.

Proposed Solutions

Technological & Political Scalability

The challenge many blockchains face when scaling is the necessity for nodes to process a full copy of the blockchain. The network therefore constantly carries with it a drag in resources spent to do the same redundant task of replicating the full blockchain.

Ouroboros instead requires only a quorum of consensus nodes to maintain the ledger with the probability proportional to the amount of coins they have.

As a cryptocurrency project grows, disagreements on philosophy or monetary policy have often lead to community fragmentation and forks, as seen with Bitcoin, Ethereum, or Litecoin. The Cardano project aims to implement a decentralized treasury where stakeholders vote on fund allocation in addition to a blockchain based system for users to propose and vote on forks.

Secure Transference of Metadata

Using a technology called Sealed Glass Proofs (SGP), the Cardano Computational Layer (CSL) will enable safe transference of personal data that is then destroyed, providing assurance that the data isn't leaked to the broader internet or kept by another entity.

Regulation Compliance Without Sacrificing Privacy

Cardano acknowledges that there are real-world situations when users are legally required to share transactional metadata, such as for tax purposes or to verify the buyer's legal age. However, it believes that the decision to share the data must rest solely with the user. The project is therefore working on adding features in its Daedalus wallet to enable users to label financial activity and share it to whoever they deem necessary. The use of Sealed Glass Proofs will guarantee that the information shared will only be used for its intended purpose and destroyed without fear that it will leak into the broader internet.

In addition, the ability to securely send data to for authentication and prove credentials should provide a global reputation system.

Cardano aims to utilize smart contracts to guarantee compliance to terms and conditions and create marketplace rules. The project's roadmap includes the creation of a decentralized autonomous organization (DAO) to add mutability to smart contracts and perform consumer protection and arbitration.

Interoperability With Other Financial Systems

The movement of value between other cryptocurrencies can be done through atomic cross chain trades or sidechains. Cardano is integrating a new KMZ sidechain protocol to safely move value between chains.

Cardano also aims to support interoperability with legacy financial systems and has identified the need to accurately represent information, value, and identities across systems. However, the challenge remains for the cryptocurrency world on how to vet the quality of information and how legacy systems can recognize value contained in cryptocurrency tokens.

Project Roadmap

The Cardano project divides its roadmap into 5 phases:

Phase 1 (Byron): bootstrapping (current phase)
Notable releases:
- Cardano Settlement Layer mainnet
- Daedelus Wallet

Phase 2 (Shelly): decentralizing the network (planned for Q2-Q3, 2018)
Notable releases:
- Delegated Ouroboros staking
- Quantum-resistant signatures
- Paper wallet support for Daedelus
- Integration with ledger wallet and debit cards

Phase 3 (Goguen): integration of smart contracts:
Notable releases:
- Sidechain support for settlement layer in preparation for connecting with the Cardano Computational Layer (CCL)
- New Haskell-like, functional code called Plutus to be used for smart contracts on CCL
- Virtual machine on CCL

Phase 4 (Basho): performance improvements
Phase 5 (Voltaire) adding a treasury system and governance

The project has deployed most of the milestones outlined in its first Byron phase, most notably having launched the Cardano Settlement Layer mainnet and the Daedelus wallet.

Roadmap Progress

Cardano has invited parties interested in running a stake pool in the Shelly testnet to register between April 5 to May 31 this year. Testnet ADA coins will be used in place of real ADA and applicants will need to be able to use a command line interface and supply and use PKI certificates.

The project is now in the process of reviewing its delegated staking feature. Once released to the Daedelus wallet, users will be able to delegate their staking responsibility to a full node so that they don't have to run a node themselves. The Daedelus staking center will display a list of public stake pools to which stake can be delegated. Users will need to pay a small fee when switching pools to protect the server from denial of service attacks.

The team is in the process of launching a testnet of its virtual machine so that the wider community can test and evaluate the implementation of smart contracts and provide feedback to the project.

New roadmap goals that have been announced include the ability to hold multiple accounts within the Daedalus wallet, thereby making inter-wallet funds easier to manage, and support for multiple currencies on the settlement and computational layer. However, both features are still in the early development stage.

Strategic Analysis

Strengths

Cardano has highly ambitious goals of becoming a universal framework for financial solutions along with a clear and extensive timeline. The project has a dedicated website outlining its extensive roadmap as well as a large archive of white papers. It is also provides regular update announcements.

As mentioned previously, the project makes sure its proposals undergo rigorous academic peer review while its functional programming language provides a high assurance for a secure protocol. This means that Cardano's blockchain will be built on one of the most highly advanced and secure languages available along with sound methodologies.

Ouroboros proof of stake is the product of combined efforts between various academic institutions.[1] The protocol has undergone extensive peer review, most notably its acceptance to the leading cryptocurrency conference Crypto 17.

Weaknesses

No project is perfect so not would be irresponsible not to mention some potential weaknesses if any are identified. In this section some of the potentially negative aspects of Cardano will be addressed.

The project's emphasis on getting it right may come at the expense of being too slow to market. In such a new industry, projects must compete for users and therefore it wouldn't matter how well designed a product is if it misses the critical adoption period for its niche. Similar projects such as NEO and EOS already have decentralized apps running on their protocols. However, these projects do not use a functional programming language. It therefore remains to be seen whether speed at the expense of security would indeed be the downfall of these competitors.

The project's updates are made according to announcement schedule and not according to the significance or sensationalism of the update. Anyone with enough experience with the cryptocurrency world knows how much of an influence news has on investor behavior and price movement.

Opportunities

Through the ability to safety transfer metadata, Cardano aims to provide legacy institutional functionality (payment system, property rights, identity, credit and risk protection, etc) for the rest of the world who don't have access to formal financial services, which is around 2 billion people according to the World Bank.

On Valentine's Day this year, open source device producer SIRIN LABS posted a Medium article announcing its strategic partnership with Cardano to integrate its FINNEY smartphone and SIRIN OS with the Cardano protocol. ADA tokens will also be supported in FINNEY's cold storage wallet and will be spendable as currency in the upcoming decentralized app store that is being developed by SIRIN LABS. This means that the ADA token will gain additional utility as an accepted currency for the SIRIN LABS decentralized app ecosystem.

1 University of Connecticut, University of Athens, University of Edinburgh, Aarhus University, Tokyo Institute of Technology.

On March 1 this year, Centra announced on its Twitter account that ADA is now a spendable asset on its prepaid card, which is currently accepted at over 36 million different locations across the world. This means that ADA is now a globally accepted cryptocurrency compared to other altcoins that struggle to find acceptance by vendors.

Cardano's startup investment arm, Emurgo, had invested in the Traxia Foundation which aims to convert invoices into tradable smart contracts. Traxia plans on migrating its platform to Cardano in Q4 in 2018 when Cardano's virtual machine goes live. Gambling platform Sp8de has also included in its roadmap plans to migrate to Cardano. These migrations to Cardano's blockchain will serve as the use-case of Cardano technology the project has been waiting for.

Furthermore, Cardano has indicated on its website that people will be able to spend ADA as currency via a Cardano debit card and be able to purchase ADA tokens at ATMs in Japan within a year of ADA's launch. However, fixed dates for these rollouts have yet to be announced.

Threats

Ethereum

Ethereum is currently by far the most popular platform for running decentralized applications. It is also headed by some of the most capable minds in the industry and will definitely not remain idle in improving its scaling capabilities. While Ethereum still uses proof of work, it is now in the process of transitioning into proof of stake, although changing such a fundamental design feature will be no simple task.

NEO

The project also uses a delegated proof of stake system similar to Cardano where holders of NEO tokens elect delegates to establish consensus on blocks. NEO is also farther ahead of Cardano in the development of its platform for decentralized apps, having already played host to a number of applications.

Where Cardano does come ahead of their competition, is the level of review and vetting the protocol has gone through. In addition, neither Ethereum nor NEO support a Haskell-based programming language which, as outlined earlier, is more thought to be more precise in ensuring the soundness of the code. In the end, the number of users, or network effect, will determine the success of a project. In other words, time will tell and it is therefore it might be wise to consider investing in Cardano's competitors as well.

Technical Analysis

Correlation with BTC

The chart above shows the price movements of ADA/BTC (blue line) and BTC/USDT (pink line) since the beginning of December last year while red line below shows the rolling 90-day correlation coefficient value between the two coins. Correlation values closer to 1 indicate a positive correlation while values closer to 0 indicate no observable correlation and values closer to -1 indicate a negative correlation.

ADA's medium correlation value with BTC/USDT of 0.4258 makes ADA a fairly diversified asset in a BTC-based portfolio.

Correlation with ETH

When examining the relationship between ADA/BTC (blue line) with ETH/USDT (green line), one can see that the two currencies have exhibited a rather correlated relationship, although the extremity of the positive relationship has slightly declined.

With a medium correlation value of 0.5692, ADA would also be considered a diversified asset when included in a ETH-based portfolio, although not as diversified as with the previous example with BTC.

Technical Forecast

From a technical perspective and depending on the timeframe, assets are either trending (up or down), or consolidating. Moving averages help us to smooth out volatile price data and provide clarity as to who controls the trend. They are by no means predictive, but can be studied to help identify the current market structure.

First is it important to note that due to Cardano being such a young asset, the available price data is extremely limited. As such, the largest timeframe we can look at is the daily level. After being listed on the exchange late last year Cardano saw an immediate and gigantic bull rally reaching almost 1300% gains, followed by a very large correction of 80% during the crash at the beginning of 2018.

As of 25-May-2018, recent price action shows that despite recent signs of new bull momentum, the market is still very much indecisive. This price action is also largely influenced by the movement of BTC, despite relatively low correlations with ADA, is still very much the dominant force in all crypto assets. We can see on the chart that short, intermediate and long moving averages continue to cross each other up and down, meaning that no clear trend has been established as of yet. Until that happens, it remains a question as to what the ultimate bottom for Cardano might end up being.

Technical Forecast (continued)

Given these current market dynamics, it's crucial not to rush into positions. Crypto assets are still highly speculative and the only thing steering projects' valuations are the everchanging inelastic forces of supply and demand. The biggest determining factor for Cardano's short to midterm success will be the outcome of the Bitcoin price over the next 4-8 weeks. Therefore, it has little use to look too much at common indicators and other things like Fibonacci levels.

Relative to the existing price history, we suggest carefully taking small positions in Cardano around the lows of the recent correction at the earliest:

Conservative entry $0.12 / 0.00001700
Aggressive entry $0.17 / 0.00002400

However, we want to stress that if the market were to steer increasingly bearish, it is not unlikely for Cardano to continue to drop lower simultaneously. For the more risk-averse investor, it may be a good idea to wait out Bitcoin's next move, and potentially risking taking a position a little higher than the targets presented here.

Of course, as usual, only invest what you can afford to lose.

Suggestions For Investment

The price of ADA has dropped to levels before the great crypto bull run last December, and therefore is trading at a significant discount for anyone wanting to bet on its success. Major exchanges that trade ADA with an English language interface are Binance and Bittrex.

The strongest argument for investing in ADA is its sober and sensible development approach that clearly distinguishes it from other projects. In an industry obsessed with speed and wrought with controversial design flaws, a project that takes such great care in ensuring security and stability is a breath of fresh air for many investors.

If one believes that a project that undertakes such rigorous peer review of proposed protocols and uses of a functional programming language for high assurance will ultimately produce most reliable foundation for decentralized apps, then one should look no further than Cardano.

- *Analysis provided by ITF Research Team.*
- *Technical Forecast provided by ITF Trader, Vinnie, who can be followed on Twitter @kingkointweet*

Disclaimers

ITF, is engaged in providing trading services to the cryptocurrency trading market. Through its bot and other services it alerts its subscribers/followers (“Users”) to certain market conditions based on those Users’ preselected settings and trading preferences. Additionally, ITF does make available, from time to time, written or electronic communications that include research analysis, and/or a opinions concerning the DLT/cryptocurrency markets (“Reports”). The views expressed in such Reports are based solely on information available publicly/ internal data/other sources believed to be true. The information is provided merely as a complementary service and do not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind.

Research data and reports published/emailed/Telegrammed/etc. and or those made available/uploaded on social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.) or disseminated in other print or electronic media by ITF, or entities with which it partners and any subsidiaries or partners thereof (“Affiliates”), or those opinions concerning cryptocurrencies expressed as and during the course of a public appearance, are for informational purposes only. Reports are provided for assistance and are not intended to, and must not, be used as the sole basis for an investment decision. The User assumes the entire risk of any use made of this information.

Reports may include projections, forecasts and other predictive statements which represent ITFs or its Affiliates’ assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. The actual performance of a company, project, token or currency represented in a Report may vary from those projected.

Disclaimers (continued)

The projections and forecasts described in any Report should be evaluated keeping in mind the fact that they:

- are based on estimates and assumptions;
- are subject to significant uncertainties and contingencies;
- will vary from actual results and such variations may increase over a period of time;
- are not scientifically proven to guarantee certain intended results;
- are not published as a warranty and do not carry any evidentiary value; and
- are not to be relied on in contractual, legal or tax advice.

Prospective investors/traders and others are cautioned that any forward-looking statements are not predictions and may be subject to change without notice. Reports based on technical analysis ("TA") are focused on studying charts and movements of a given currency or token's price movement and/or trading volume. As such, a Report based on TA may not match with a Report on fundamental analysis. Though Reports are reviewed for any untrue statements of material facts or any false or misleading information, ITF does not represent that ANY REPORT is accurate or complete and again emphasizes that NO REPORT should be relied on in connection with a purchase, investment, commitment, or contract by anyone whatsoever. ITF does not guarantee the accuracy, adequacy, completeness or availability of any information in any Report and therefore CANNOT be held responsible for any errors or omissions or for the results obtained from the use of such information. ITF, its Affiliates and the officers, directors, and employees of either, including analysts/authors shall not be in any way responsible for any direct, indirect, special or consequential damages that may befall any person from any information contained in any Report nor do they guarantee or assume liability for any omission of information from therein. Information contained in any Report cannot be the basis for any claim, demand or cause of action. These data, Reports, and information do not constitute scientific publications and do not carry any evidentiary value whatsoever.

ITF's Reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and/or ITF Reports, in any form, is prohibited except with the written permission of ITF. Persons into whose possession the Reports may come are required to observe these restrictions. Opinions expressed therein are current as of the date appearing on the report only. Data may be subject to update and correction without notice. While ITF endeavors to update (on a reasonable basis) the information discussed in the Reports, there may be regulatory, compliance, or other reasons that prevent ITF from doing so.

The Reports do not take into account the particular investment objectives, financial situations, risk profile or needs of any person, natural or otherwise. The User assumes the entire risk of any use made of this information. Each recipient of a Report should make such investigation as deemed necessary to arrive at an independent evaluation of an acquisition of the asset referred to in any Report (including the merits and risks involved).

Cryptocurrencies involve substantial risks and are not suitable for all investors/traders. Investors can lose their entire investment relatively easily in the cryptocurrency markets. Before acting on any advice or recommendation in this material, Users should consider whether it is suitable for their particular circumstances and, if necessary, seek professional advice. The price and value of investments referred to in research reports and the income from them may fluctuate.

Disclaimers (continued)

Certain information set forth in this Report contains "forward-looking information", including "future oriented financial information" and "financial outlook", under potentially applicable securities laws (collectively referred to herein as "Forward-Looking Statements"). Except for statements of historical fact, information contained herein constitutes Forward-Looking Statements and includes, but is not limited to, the (i) projected financial performance of a company, project, token, or currency; (ii) completion of, and the use of proceeds from, the sale of tokens being offered to the public; (iii) the expected development of a company, project, token, or currency's business, projects and joint ventures; (iv) execution of the company's or the project, token, or currency's developers' vision and growth strategy; (v) sources and availability of funding for the company, project, token, or currency; (vi) completion of any projects that are currently underway, in development or otherwise under consideration; (vi) renewal of any material agreements; and (vii) future liquidity, working capital, and capital requirements. Forward-Looking Statements are provided to allow potential investors the opportunity to understand ITF's beliefs and opinions in respect to the future of a given company, project, token, or currency so that they may use such beliefs and opinions as one factor in evaluating an investment.

NO statement issued on ITF's website or in any Report is a guarantee of future performance and undue reliance should not be placed on them. Such Forward-Looking Statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although Forward-Looking Statements contained in this presentation are based upon what ITF and/or its Affiliates believe are reasonable assumptions, there can be no assurance that Forward-Looking Statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Neither ITF nor any of its Affiliates undertake any obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable laws. The User is cautioned not to place undue reliance on forward-looking statements.

The User should consult their own advisors to determine the merits and risks of ANY investment.