N·K·B
BLOCKCHAIN INVESTMENT & ADVISORY

Sector: Infrastructure

Cardano Review 25 June 2018

- Cardano is developing an open-source smart contract platform, which aims to deliver more advanced features than other existing platforms. The project incorporates a research-driven approach.
- The blockchain uses Ouroboros Proof-of-Stake (POS) protocol, which provides faster and cheaper transactions compared to Proof-of-Work, and offers a novel reward mechanism for incentivizing POS in that it neutralizes attacks such as selfish mining. The platform is adaptive and does not require much forking to make amendments. Two layers implemented within Cardano allow the application to meet regulatory requirements, including KYC, AML and other regulation required to run apps.
- Cardano is developed by the IOHK team, led by Charles Hoskinson, a former co-founder of BitShares, Invictus Innovations and ex-CEO of Ethereum and Ethereum Classic, alongside Jeremy Wood, a former Ethereum team member. The Cardano project flow is run by a very skilled team across several countries, including representatives of various universities. Cardano has one of the largest networks, including developers and followers on social media.
- The Cardano blockchain was launched in September 2017. Currently, the team is working to launch smart contracts in Q4 2018. Use cases for Cardano include gaming, gambling, register, payments, and other applications as well as an ICO platform. The blockchain may become fully decentralised in 2019, once the team completes the next implementation phase.
- Risks include a possible long implementation period that allows competitive projects to win some market share; low adoption by the developers; regulatory changes and more.

Date	**25 June 2018**
Token	ADA
Circulating supply	25,927,070,538
Total supply	31,112,483,745
Max supply	45,000,000,000
Price, $	0.136
MktCap, $m	3,527

Research Analysts:

Marina Alekseenkova
Marina.Alekseenkova@nkbgroup.io
David Arvay
David.Arvay@nkbgroup.io

Description

The Cardano decentralised blockchain is an open source platform which uses a proof-of-stake algorithm called Ouroboros. The algorithm has consensus generated by coin-holder voting. Slot leaders, who hold a native platform coin ADA, generate new blocks in the blockchain and confirm the transactions. The Cardano blockchain has two main layers: 1) ADA cryptocurrency which operates on the Cardano Settlement Layer (CSL), and which is a ledger supporting transactions; 2) The Cardano Computation Layer (CCL) which supports smart contracts and decentralised applications. The Cardano blockchain maybe easier to update via soft forks compared to Ethereum, which has those two layers intertwined. The two layers CSL and CCL are connected by side chains. Cardano uses the Haskell programming language with a high degree of fault tolerance. The ADA cryptocurrency is developed around a Recursive InterNetwork Architecture (RINA). The Cardano blockchain was released on 29 September 2017. The team is located in Japan, USA, and Hong Kong.

Cardano Settlement Layer

Cardano SL (or Cardano Settlement Layer) is a cryptographic currency designed and developed by Input-Output Hong Kong (IOHK) in conjunction with the University of Edinburgh, the University of Athens and the University of Connecticut. The Cardano team has developed the secured proof-of-stake algorithm called Ouroboros. The main idea of the **Ouroboros** proof-of-stake protocol is that a node is selected to make a new block, with a probability proportional to the amount of coins this node has. If a node has a positive stake (>0), it is called a stakeholder. If a node is chosen to make block it is called a slot leader.

Nodes with a positive stake called **stakeholders** and only stakeholders may participate in running the protocol. A stakeholder must be elected as a **slot leader** to be able to generate new blocks for the blockchain. The slot leader can listen to transactions announced by other nodes, make a block of those transactions, sign this block with its secret key, and publish it to the network.

The Ouroboros protocol divides the physical time into **epochs**, and each epoch is divided into **slots** (short periods, c.20 seconds). Each slot has only one slot leader (SL). A slot leader has a right to produce only one block during their slot. The number of slot leaders is equal to the number of slots in the epoch (N), and it is impossible to produce more than N blocks during an epoch. One or more slots can remain empty but the majority of blocks (50%+1) must be generated during an epoch.

Slot leaders are elected from the group of all stakeholders. The voting in the election is allowed only for those stakeholders who have enough stake (2% of the total stake). This group of stakeholders is called **electors**. Electors elect the slot leaders for the next epoch during the current epoch. The more stake a stakeholder has, the more chances one has to be elected as a slot leader. During the slot leader election, a certain degree of randomness is needed as a base for election. To make it possible, a **multiparty computation (MPC)** approach is used to achieve this randomness where each elector independently performs an action called “coin tossing” and after that, they share results with other electors. An elector generates a secret random value, then forms a “commitment” which is a message that contains encrypted shares and proof of secret. At the next step, an elector signs this commitment with its secret key, specifies the epoch’s number and attaches its public key. That allows everyone to know who created this commitment. Those commitments are put into the block and become a part of the blockchain. The reveal phase is when an elector sends an “opening”, that involves a key that opens the

commitment. The final phase of the process is called the recovery phase. An elector has both commitments and openings. The honest electors can post all shares to reconstruct the secret. An election finishes successfully even if some electors are adversaries. An elector verifies that commitments and openings match and extracts the secrets from the commitments and forms a seed from these secrets. All electors get the same seed and it is used for the **Follow the Satoshi (FTS)** algorithm.

Once electors have the seed, they have to select slot leaders for the next epoch. It is also achieved with the Follow the Satoshi algorithm. FTS is an algorithm that verifiably picks a coin, and when coin owned by stakeholder S is selected, S becomes a slot leader. The more coins the stakeholder has, the higher probability of one of their coins being selected. Honest majority assumes that participants owning at least 50%+1 of the total stake are honest ones.

The Cardano SL has been amended versus what was stated in the White paper, as the PVSS (Publicly Verifiable Secret Sharing) was replaced with Scalable Randomness, as attested by public entities. The Cardano SL introduced a special constant called the "**network diameter**" which is the maximum time necessary to broadcast a block to all nodes in the network. Some further implementations and modifications have been undertaken, which are not in the whitepaper.

There are two concepts used in the Cardano SL: 1) **balance** is the real amount of coins that each user has, and 2) **stake** is a user's ability to control the actual Cardano SL. The relation between balance and stake may be changed via stake delegation. Stake gives a user the power to control various Candano SL parts, including being a slot leader, voting in the update system and taking part in MPC/SSC. The Cardano protocol will be updated using stakes for voting for soft and hard forks.

The **topology** of the Cardano network includes **three groups of nodes**: 1) **core** nodes - the most important nodes which can be slot leaders and create new blocks, but never create currency transactions, 2) **relay** nodes – which are the proxy between the core nodes and the public internet, which do not have any stake so can be moved, cannot be slot leaders, cannot create currency transactions, they are under the control of the federated committee of initial stakeholders, 3) **edge** nodes – which are simple nodes that anyone can run on the computer, can create currency transactions, cannot be slot leaders, and which cannot directly communicate with core nodes but only with relay nodes.

The Cardano SL is the first component of the Cardano platform and called a layer. It is expanded with a control layer to evaluate a special kind of proof to ensure that a certain computation is carried out correctly. Such systems are used in identity management, credit system, gaming and gambling, and others.

Cardano Roadmap

The Cardano timeline is divided into three periods:

- **Testnet era:** all functionality, including the reward mechanism, is activated; all participants test the network by downloading software and providing feedback;
- **Byron phase or Bootstrap era:** the network operates in "bootstrap mode", people who purchased ADA redeem their coins, the stake will automatically get delegated to a pool of trusted nodes that will maintain a network. During this period no block rewards will be issued. The network is currently operating in Bootstrap mode;
- **Shelley phase or Reward era:** a normal operation mode of the network.

Figure 1. Cardano Roadmap

Cardano SL Mainnet Launch	**29 September 2017**
Byron Phase – current	Following two years of research, IOHK has designed a cryptocurrency technology, which is now in the Byron phase (bootstrap era). The main purpose of this phase is to make Cardano SL completely decentralised. The main focus will be on the networking layer, on making Ouroboros more robust, on multisignature addresses, light clients, quantum resistant signatures and other add-ons.
Shelley Phase	The Shelley phase focuses on ensuring that all the elements are in place for the technology to grow into a fully decentralised and autonomous system . **Shelley features are to be released in Q2-Q3 2018.** The list of features includes delegation and stake pool testnets. **Open Ouroboros delegation** is a process when users are able to delegate their stake or to act as stake pools and have stake delegated to them. **Multisignature** transactions will be supported for HD wallets (35% done) **Wallet backend** will be redesigned to improve performance (65% done) **Consensus incentives** and fees in Cardano will be used to encourage shareholders to set up the infrastructure needed to run a full node and to fully participate in the protocol (80% done) **Quantum resistant signatures** will be added (50% progress). **Light client** support will enable faster blockchain syncing by subscribing to checkpoints, snapshots of the Cardano blockchain in time (20% done) **Human-friendly addresses** are significantly shorter addresses that will be displayed in the user interface. **Networking** includes wide network topography enabling decentralisation without sacrificing performance or security (55% done) **Paper wallets** for Daedalus (85% done) **Daedalus wallet accounts** will be able to hold multiple accounts (20% done) **Ledger wallet** with debit cards.
Goguen	The new generation **virtual machine IELE** and universal language framework were designed as core infrastructure for future blockchain technologies. **Sidechains** will allow the addition of new features without forking a blockchain (75% done). **Accounting model** to move value between ledgers will be developed (60% done). **Multi-currency ledger** will be designed to support multiple currencies (20% done)
Plutus	**Plutus language** will be finalised and integrated into the Cardano SL. **Plutus** is a programming language used for defining smart contracts in Cardano. The syntax is fairly Haskell-like but more evaluated compared to Haskell. **IELE Virtual Machine VI** will be created (75% done) **Integration and Implementation** of the sidechains and accounting will be completed in the SL and CL, IELE and Plutus Core will be integrated into the CL (15% done)

	Smart contracts deployment and integration, including a set of tools, will be available for development of smart contracts (early development). Goguen testnet was planned to launch in May 2018, **IELE Virtual Machine** testnet will be launched in **Jul 2018**.
Basho	The feature of Basho is focused on performance improvement, scalability, and security.
Voltaire	**Voltaire** will be focused on assurance and scalability and will introduce a treasury model.

Source: Cardano technical papers and website

So, there are few milestones promised by the team in 2018, including the release of the IELE virtual machine in Jul 2018, and the Goguen project with smart contracts release in Q418, plus a general update and Shelley releases in Q2-3 2018.

Cardano Use Cases

The Cardano platform allows a wide range of applications to be run on the platform. The essential infrastructure is under development, however, the sustainable research-driven approach by IOHK will allow the essential part of the infrastructure to be ready in 2018. The team is aiming to evolve Daedalus, the Cardano SL wallet application, into a universal cryptocurrency wallet featuring automated cryptocurrency trading and cryptocurrency-to-fiat transactions.

There are several use cases under development on the Cardano platform:

- Proof of university diplomas in Greece, a joint project with the national research and education network of Greece GRNET, is the first use case for Cardano. The use case of a register may be developed widely, given the compliance layer of the platform.
- Cardano planned initial smart contract applications such as a casino and an integration with the mobile gaming market, in its ICO documentation.
- Cardano debit cards are planned in the roadmap to provide users with ADA available everywhere.
- The first ICO which can potentially use Cardano was launched in March 2018. Traxia is creating a decentralized global trade finance system where invoices are converted into smart contracts and traded as short-term assets. The Traxia project is currently built on Ethereum technology but will be migrating to Cardano in Q4 2018, when Cardano's Goguen goes live.

Cardano Monetary Policy

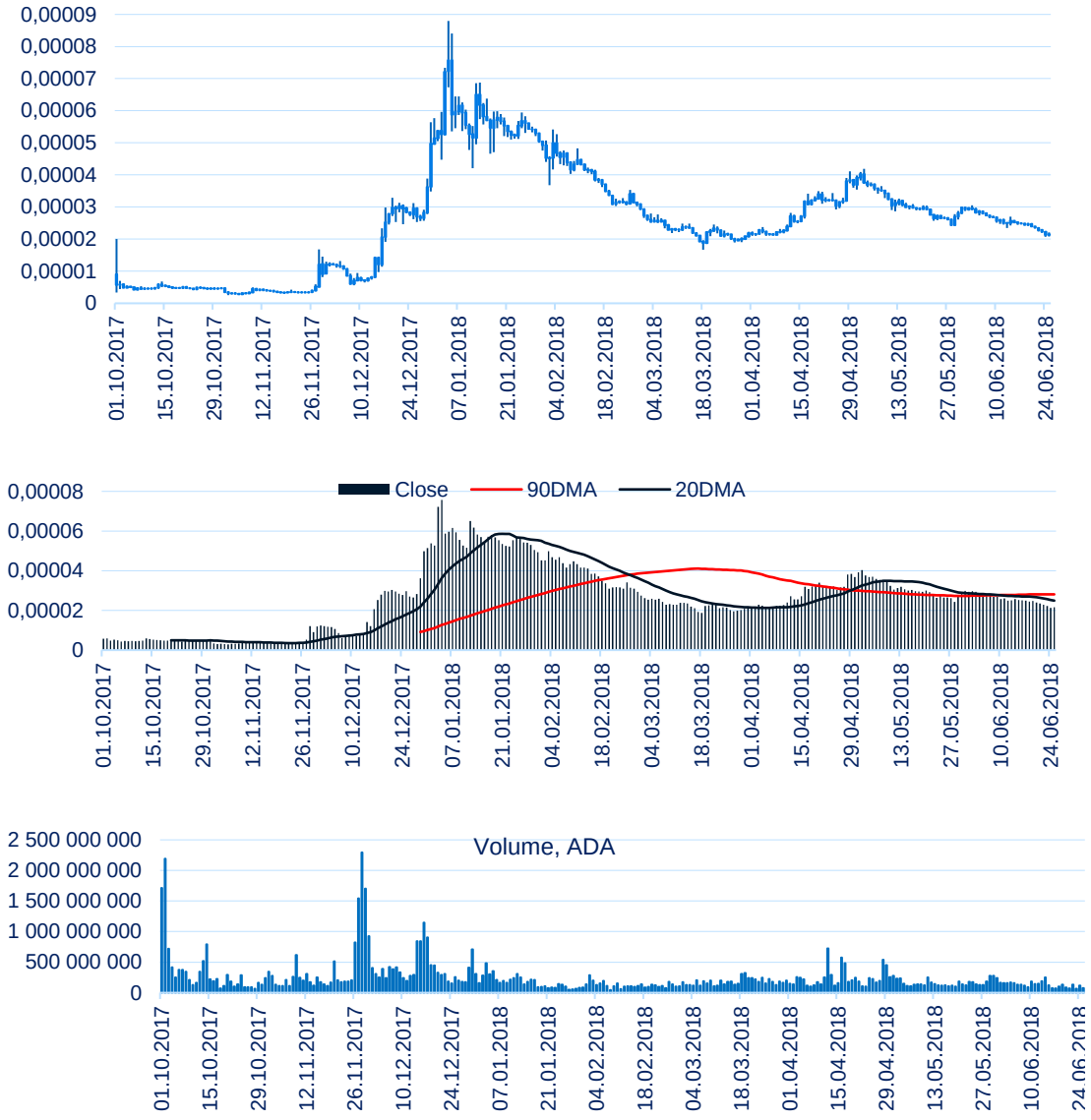
At the launch of Cardano, it was sold for 25,927,070,538 ADA tokens. There were 5,185,414,108 vouchers distributed to three entities of the Cardano community - IOHK, Emurgo, and the Cardano Foundation, making the total amount of ADA available at the launch as 31,112,484,646 ADA. ADA tokens are capped at an arbitrary 45,000,000,000 ADA. There are 13,887,515,354 ADA to be issued after the launch through mining. One ADA equals 1,000,000 Lovelaces. ADA has six decimal places. The ADA token is named after Augusta Ada King-Noel, Countess of Lovelace (nee Byron), an English mathematician known for her work on Charles Babbage's proposed mechanical general-purpose computer, the Analytical Engine. The Cardano blockchain is named after Gerolamo Cardano, an Italian polymath famous for his work on probability, binomial coefficients, and binomial theorem.
Cardano is at the bootstrapping phase when fees are not collected and no ADA is being minted. Fees from this phase will be collected in the future and they will be destroyed. In the future, Cardano will have

treasury funded with newly-minted ADA and transaction fees. The treasury will be governed by ADA holders.
The minimal fee at the Cardano blockchain is defined as 0.155381 ADA plus 0.000043946 ADA/Byte multiplied by the size of the transaction. The formula for the fee calculation is not the final one as the team is researching this area and some amendments might be implemented.

Cardano ICO

The Cardano ICO took place between September 2015 and January 2017 with KYC requirements applied. The investment base of Cardano ICOs includes primarily Japanese (95%), Korean (2.56%) and Chinese (2.39%) investors. The amount of sold tokens was 26,000,000,000 out of 45,000,000,000 ADA. The project raised c.$63m, which translates to an average price of $0.00242 per ADA, and a market capitalisation of $109mn after the ICO.

Figure 2. ADA token price, BTC/ADA



Source: Cryptocompare.com, NKB Research

Team

The Cardano blockchain is built around three entities:

The Cardano Foundation, which is a promoter, educator and standard body for the blockchain and its apps. The foundation provides a formal specification and standardization process.

Input Output Hong Kong (IOHK) is the founder and the engineering company which designs the platform. IOHK has a strong team and designs the protocol. Two co-founders of IOHK are Charles Hoskinson, formerly the CEO of the Ethereum project in Dec 2013 – May 2014 and founder of Invictus Innovations and IOHK. Jeremy Wood was managing operations in Ethereum at the end of 2013, and jointly with Charles Hoskinson founded Input Output Hong Kong in 2015.

Emurgo, a business partner of the project will incentivize growth on Cardano by funding start-ups building dApps on the blockchain.

The Cardano project flow is run by a very skilled team across multiple countries, including representatives of several universities. Cardano has one of the largest networks, including developers and followers on social media.

Figure 3. Number of subscribers

	Reddit	Github, commits	Twitter, followers	Youtube, subscribers
Cardano	65,110 subscribers, 2339 active users, 82 comments/day	14,300	118830	20,000
EOS	51,310 subscribers, 3,373 active users, 1567 comments/day	7,544 commits	166,090	12,000
Ethereum	365,500 subscribers, 4284 active users, 300 comments/day	224,000	398,830	54,000

Source: cryptocompare.com, youtube, reddit, github, twitter

The sentiment around Cardano is very optimistic, compared to other platforms. The social media posts mostly confirm that users and followers are generally assuming that Cardano is one of the most prominent platforms.

There are several concerns:

- The heavy academic approach may result in a delay of the project with other less technologically prominent projects taking over the market share.
- The whitepaper and Cardano website promise many different features, some of them may be hard to realise.

However, the general impression of the community remains positive.

Comparison of Blockchain Platforms

The Cardano protocol is aiming to provide a superior processing capacity of the network in terms of the number of transactions. The design of the Omniboros POS protocol also assumes high security compared to other POS protocols. Thus, scalability and security, as well as low cost, make this blockchain a good option for the decentralised apps as well as a payment system. Compared to other POS-based blockchains, Cardano also has an additional layer which allows implementation of regulatory requirements.

The transition of Ethereum, the platform which currently dominates the ICO market, from POW to POS (Ethereum's Casper has already been released as a link between POW and POS), represents a potential risk for other platforms under development. Ethereum has the widest adoption among platforms and many projects use software already created on Ethereum that essentially eases the development of new projects.

Figure 4. Comparison of blockchain platforms

	TON	Bitcoin	Ethereum	NXT	Tezos	Casper	Bitshares	Cardano	EOS	PolkaDot	Cosmos
Announced	2017	2009	2013, 2015	2014	2017	2015	2013, 2014	2015	2016	2016	2017
Deployed	2018					2017		2017	2018	2019	
Consensus	POS BFT	POW	POW	POS	POS	POW/ POS	DPoS	POS/ DPoS	DPoS	PoS BFT	PoS BFT
Smart contract	Yes	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Blockchain type Single (1)/ Multiple (M)	M	1	1	1	1	1	M	M	M	M	M
Multichain Heterogeneous (Ht) /Homogeneous	Mix						Ht	Ht	Ht	Ht	Ht
Sharding support	Dyna mic						No	No	No	No	No
Interaction between blockchains	Tight						Loose	NA	Loose	Loose	Loose

Source: TON Technical paper, companies' data

Figure 5. Key parameters of the blockchain platforms

as of 25 June 2018	Number of transactions per second	MktCap, $m	Volume (24H), $m	Processed value per year, $m	MktCap/ Volume	Average velocity
Bitcoin	7	106081	4175	1 523 824	6,96%	14,4
Ethereum	15	46054	2390	872 456	5,28%	18,9
Stellar	1500	3611	36	13 231	27,29%	3,7
EOS	1000	7375	1097	400 372	1,84%	54,3
Bitshares	1500	356	10	3 639	9,78%	10,2
Cardano	10	3487	56	20 436	17,06%	5,9
Ripple	1500	19117	277	100 942	18,94%	5,3
NEO	1000	2061	71	25 945	7,94%	12,6

*Source: Coinmarketcap.com, Hypothesis Research estimates, *) Testnet*

Risks

- The regulatory environment may change over time, implying a different requirement for the platform.
- Delay with the development creates a pressure from competitive projects.
- Adoption of the blockchain by developers may be slow
- Technical implementation of all announced features may be delayed or not realised in full.
- ADA token may lose its value.
- The governance system may modify the initially proposed blockchain.

Sources

https://cardanodocs.com/glossary/
https://daedaluswallet.io/
https://cardanofoundation.org/foundation/
https://github.com/input-output-hk/cardano-sl
https://discordapp.com/invite/27KvYjS
https://twitter.com/@InputOutputHK
https://www.cardano.org/ja/audit-report-summary-2/
https://www.cardano.org/en/genesis-block-distribution/
https://iohk.io/projects/cardano/#team
https://steemit.com/cryptocurrency/@nrek/the-real-next-neo-is-here-meet-cardano-and-ada

ANALYSTS CERTIFICATION AND DISCLAIMER

This report has been prepared and issued by Hypothesis Research Limited ("Hypothesis") in accordance with Hypothesis policies for managing conflicts of interest arising as a result of publication and distribution of investment research. Hypothesis is authorised and regulated by the Financial Conduct Authority ("FCA"). This report has been prepared by the analyst whose name appears on the front page of this report.

The information contained within the report is intended for use by professional clients and eligible counterparties as defined in section 3 of the FCA Conduct of Business rules. Our research must not be acted on or relied upon by persons in the UK who would be categorised as retail clients.

The report must not be distributed in any other jurisdictions where its distribution may be restricted by law. Persons into whose possession this report comes into should inform themselves about, and observe, any such restrictions.

All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report. Opinions contained in this report represent those of Hypothesis and the analyst at the time of publication.

Hypothesis does not offer or provide personalised advice. The information provided is not intended to be, and should not be construed in any manner whatsoever as, personalised advice as it does not have regard to the specific investment objectives, financial situation and particular needs of any specific person who may receive this report. The information provided by us should not be construed by any subscriber or prospective subscriber as Hypothesis' solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned in this report. Investors should make their own investment decisions based upon their own financial objective and resources.

Hypothesis has a restrictive policy relating to personal dealing. Hypothesis, its respective directors, officers, employees and contractors do not hold any positions in the securities mentioned in this report. Hypothesis may perform services or solicit business from any of the companies mentioned in this report.

The value of securities mentioned in this report can fall as well as rise and may be subject to large and sudden swings. In addition, it may be difficult or not possible to buy, sell or obtain accurate information about the value of securities mentioned in this report. Past performance is not necessarily a guide to future performance. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

To the maximum extent permitted by law, Hypothesis, its affiliates and contractors, and their respective directors, officers and employees will not be liable for any loss or damage arising as a result of reliance being placed on any of the information contained in this report and do not guarantee the returns on investments in the products discussed in this publication.

NKB Group

Offices: London, Vienna

www.nkbgroup.io

The report is prepared by NKB Group in collaboration with Hypothesis Research Ltd (UK).