# THE CASE FOR CARDANO



Prepared by Jacob Koch-Gallup June 13<sup>th</sup>, 2021



+

C

# Facts about Cardano

Founded by Ethereum's Co-founder, Charles Hoskinson, in 2015

Launched in 2017 by Hoskinson's company IOHK

Cardano relies on Proof of Stake protocols

Cardano's ADA tokens have a strict cap of 45 billion tokens

Currently, almost 32 billion tokens have been mined

Cardano's Market Cap is almost \$50 billion at \$1.54 per ADA token

Currently #5 in Market Cap behind Bitcoin, Ethereum, Tether, and Binance Coin



# Cardano's Potential

Used peer-reviewed scientific research to build its platform

Faster speeds than most other blockchains

Less energy usage than most other blockchains

Focus on governments to expand globally

# Peer-Reviewed Scientific Research

#### Ouroboros-BFT A Simple Byzantine Fault Tolerant Consensus Protocol

Applie Kayior Alexander Bassell! November 26, 2018

We present a single, detectable period for high respect that the first interest that the first first first and the single period by the present of the first first

The consension problems, throulesed by restrict work of floatists. Done and Lampers [10, 10], is out at the Indianceoid problems in empirice reviews. The problem has neverted account from the low decased do not applicate in computer reviews. The problem has neverted account from the low decase do not applicate in configurations and the low of the low of the problems of the low [11]. Since the delity to indiant particular advantages the low floating the low decast country and the configuration by an indemnification of the problems of the indiant decast lower through the low decast country and the configuration by an indemnification of the problems of the indiant low decast low decast country and the low of the low decast low of the problems of the low of the low decast lo

Description JPT is a new RPT indeer recognized prescript by the design of the Ozenhana

princed [7], a pred of able trickhold proteind. Outdoors IIIT is a fitterwise the princed with this philips of the princed with the the in the synchroneous secting, though we also show that it is redificit to synchrony distinct modifies two action natural with an examination of supervision and the natural synchronic processing the substitution continues in motion. The generating provides between the substitution in the sense that

to taken state of the legacy and 1990. At applicability of the month was partially experted by 1990 property PAPVALIGIDE at Polish's and Expropriety ATD.

\*\*University of Connection and MOSE, northern contention.

#### Proof-of-Stake Sidechains

Peter Gazi<sup>1</sup>, Aggelos Kinyias<sup>1,2</sup>, and Dionysis Zindros<sup>1,3</sup>

1 IOHK <sup>2</sup> University of Edinburgh National and Kapodistrian University of Athens

December 18, 2018

Abstract. Sideclains have long been beralded as the key enabler of blockchain acalability and interoperability. However, no modeling of the concept or a provably secure construction has so far been

We provide the first formal definition of what a advehage motion is and how assets can be moved between sidechains securely. We put forth a security definition that augments the known transaction ledger properties of persistence and liveness to hold across multiple ledgers and enhance there with a new "firewall" occurity property which safeguards each blockchain from its sidechains, limiting the

impset of an otherwise estastrophic aidechain failum.

We then provide a sidechain construction that it suitable for proof-of-stake (PoS) sidechain systems. As an exemplary concross instantiation we present our construction for an epoch-based PoS system. consistent with Ouroboros (Crypto 2017), the PoS blockchain protocol used in Cardano which is one of the largest pure PoS systems by market capitalization, and we also comment how the construction ean be adapted for other protocols such as Ouroboros Prace (Eurocrypt 2018), Ouroboros Cenesis (CCS 2018). Snow White and Algorand. An important feature of our construction is merged-staking that prevents "goldlinger" attacks against a sickednin that is only carrying a small amount of stake. An important technique for pegging simins that we use in our construction is cross-chain certification which is socilitated by a novel cryptographic primitive we introduce called ad-hoc threshold multisegnatures (ATMS) which may be of independent interest. We show how ATMS can be securely instantiated by regular and aggregate digital signatures as well as succinct arguments of knowledge such as STAIUA and bulletproofs with varying degrees of storage efficiency.

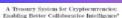
Blockshain protocols and their most prominent application so far, cryptocurrencies like Bitcoin [27], have been gaining increasing popularity and acceptance by a wider community. While ergoging wide adoption, there are several fundamental open questions remaining to be resolved that include (i) Interoperability. How can different blockchains interoperate and exchange assets or other data? (ii) Scalability: How can blockchain protocols scale, especially proportionally to the number of participating nodes? (iii) Upgradability: How can a deployed blockehain protocol codebase evolve to support a new functionality, or correct an implementation

The main function of a blockchain protocol is to organize application data into blocks so that a set of nodes that evolves over time can arrive eventually to consensus about the sequence of events that took place The consensus component can be achieved in a number of ways, the most popular is using proof-of-work III (cf. [27,177]), while a promising alternative is to use proof-of-stake (cf. [25,23,5173]). Application data typically consists of transactions indicating some transfer of value as in the case of Bitcoin [25]. The transfer of value

can be conditioned on arbitrary predicates called swart contracts such as, for example, in Ethereum [HES].

The conditions used to validate transactions depend on local blockshain events according to the view of each node and they typically cannot be dependent on other blockchain sessions. Being able to perform operations across blockchains, for instance from a main blockchain such as Bitcom to a "sideclasm" that has some enhanced functionality, has been frequently considered a fundamental technology enabler in the

A See a.g., https://blockstream.com/technology/ sod [].



#### University of Edinburgh

#### University of Athens

**Lancaster University** 

University of Connecticut

> https://eprint.iacr.org/2018/1049.pdf https://eprint.iacr.org/2018/435.pdf https://eprint.iacr.org/2018/1239.pdf

# Faster Speeds



+

	Ripple	Lite coin	Bitcoin	Bitcoin Cash	Bitcoin SV	Ethereum	Ethereum 2.0 (not occurring until late 2021 or 2022)	Cardano
Approximate transactions per second (TPS)	15,000 TPS	56 TPS	4-7 TPS	300 TPS	224 TPS	15-30 TPS	10,000 TPS	Up to 1 million TPS  (w/ Hydra Ouroboros, but currently capped at 6.5 TPS based on demand)



# Less Energy



			Ξ	

	Ripple	Litecoin	Bitcoin Cash	Bitcoin SV	Bitcoin	Ethereum	Ethereum 2.0 (not occurring until late 2021 or 2022)	Cardano
TWh consumpution annually	0.004744 TWh	3.2 TWh	3.4 TWh	<1 TWh	114 TWh	44 TWh	0.0053 TWh	0.006 TWh
kWh consumption per transaction	0.0079 kWh	18.522 kWh	18.957 kWh	Data Unavailable	1568.86 kWh	113.71 kWh	.035 kWh	0.5479 kWh

+

0

https://www.tomsguide.com/news/ethereum-crypto-will-soon-be-9995-more-environmentally-friendly-heres-howhttps://digiconomist.net/bitcoin-energy-consumption

https://digiconomist.net/ethereum-energy-consumption

tps://ca.finance.yahoo.com/news/forget-bitcoin-dogecoin-ethereum-cardano-193020981.html

https://forum.cardano.org/t/how-cardano-uses-significantly-less-energy-while-maintaining-the-same-level-of-security-as-bitcoin/62629

https://www.laptopmag.com/best-picks/most-energy-efficient-cryptocurrencies-the-best-picks-for-teslas-new-coin

https://www.cryptovantage.com/news/what-are-the-top-10-greenest-cryptocurrencies-you-might-be-surprise

### Cardano's Focus on Governments



#### Ethiopian Education System

Cardano partnered with the Ethiopian government to transform the education system using their smart contract platform.

Students across Ethiopia will be given a digital identity (DID). This metadata will carry all information regarding the student's academic performance throughout school.

5 million students and 700,000 teachers from 3,500 schools across Ethiopia using Atala PRISM (Cardano's decentralized identity solution technology) are currently being integrated with the Cardano blockchain.

When these millions of students graduate, as they go into the economy, Cardano's hope is for this infrastructure to be used for buying property, for payments, for voting and any other economic matters.

#### Tanzanian Infrastructure

Cardano partnered with World Mobile Group to bring sustainable internet connectivity using renewable, solar-powered energy to Tanzania.

Together, the companies will provide affordable network nodes, based on Cardano's blockchain infrastructure, to local business owners. These network nodes will act as local relays for internet connectivity.

Subscribers to these networks will be able to access Atala PRISM, providing services such as digital banking, healthcare, and education.

#### Ask The Doctor

Ask The Doctor, a global digital healthcare platform, announced in March that it will switch its AskToken to Cardano.

The AskToken will first be deployed in Africa, before launching in other parts of the world.

The AskToken is currently an ERC-20 utility token on the Ethereum blockchain.

Ask The Doctor enables users to earn crypto by learning about basic healthcare. They can then use what they've earned to pay for doctors and medication.

