Institution: University of Edinburgh

Unit of Assessment: 11

Title of case study: Ouroboros provable proof-of-stake protocol ensures success of new blockchain platform and cryptocurrency

Period when the underpinning research was undertaken: 2016 – 2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Aggelos Kiayias	Professor	2015 – present
Markulf Kohlweiss	Senior Lecturer	2018 – present
Vassilis Zikas	Senior Lecturer	2018 – present

Period when the claimed impact occurred: 2017 – 2020

Is this case study continued from a case study submitted in 2014? No

1. Summary of the impact

Research at the University of Edinburgh has resulted in the first ever mathematically provable proof-of-stake protocol for use in blockchain and distributed ledger technology. Named Ouroboros, it has been adopted by technology company Input Output Hong Kong (IOHK) to underpin the blockchain platform Cardano and related cryptocurrency Cardano ADA. The Cardano blockchain has also been acquired for use in public and economic services in several countries, including Georgia, where it is now used to verify degree certificates. Cardano ADA has thrived on the reputation of its security, and has been directly credited by IOHK in generating [text removed for publication] in new contracts, and in increasing the company's size elevenfold. Ouroboros enables Cardano to operate at a unique level of impenetrability, while substantially reducing the energy expenditure usually required for such security.

2. Underpinning research

There are many applications of distributed ledger technology (DLT). Notably using DLT it is possible to compute any multiparty functionality securely, fairly and robustly as shown in [3.1]. Proof-of-work (PoW) blockchain protocols have long been the only provably secure method to obtain large scale permissionless DLT. While secure and resistant to hacking, such protocols are very energy-expensive. At the time of writing, the Bitcoin (PoW) blockchain consumes over 60 TWhr per year, a level of energy consumption that is on par with that of a medium sized European country, such as Austria or Czechia (https://www.cbeci.org/). By contrast, proof-of-stake (PoS) protocols were conjectured to have the potential to be far more energy-efficient (summarised in [3.2]). The reduced computational power requirements for PoS protocols allow for increased decentralisation, since resource holders do not need to be concentrated in geographic areas with preferential energy tariffs. This means that the overall blockchain is less susceptible to manipulation – the more stake pools there are, the more difficult it is for one malicious user ("adversary") to hold >50% of the resources needed to engage in the protocol and thus corrupt the blockchain. However, until the Ouroboros protocol was published by Edinburgh researchers in 2017, no PoS protocol had been demonstrated to have rigorous security guarantees.

The Ouroboros protocol [3.2] is the first provably secure PoS protocol to pass per review. The development of Ouroboros was led by Aggelos Kiayias (Chair in Cybersecurity and Privacy) at the University of Edinburgh, and was partly supported by the H2020 project

PANORAMIX (01/09/2015 – 31/01/2019). As a PoS protocol, Ouroboros also addresses the issue of energy-expensive secure protocols.

In PoS protocols, the selection of the next block "leader" is based on stake rather than computational power. In Ouroboros, stake is assumed to change over time, accurately reflecting that participants hold varying stake over time. To fairly select the next leader, the Ouroboros protocol divides protocol time into epochs and regularly "pumps" unbiased randomness into the blockchain using a suitably designed coin-flipping protocol. This protocol architecture enabled the development of a formal mathematical argument that established the protocol's security properties along the same lines as that of the Bitcoin blockchain for the first time.

Subsequent research efforts were then made to refine the protocol, and to provide security against stronger adversarial models encompassing an even wider set of potential real world attacks, resulting in the creation of Ouroboros Praos [3.3]. Where before an adversary could take advantage of tight synchronicity failures and focus attack resources on upcoming stakeholders in the protocol schedule, Ouroboros Praos ensures that none of these threats can materialise.

Further research into the robustness of Ouroboros and other PoS protocols demonstrated vulnerability of such protocols to so-called "stake-bleeding" attacks, which exploit long-running blockchain operations and thus need to be taken into account in order to future-proof PoS protocols [3.4]. Following this research, the team continued work on the Ouroboros protocol, ensuring that the next-generation Ouroboros protocol (Ouroboros Genesis) could enable bootstrapping clients, (i.e. clients joining the network for the first time) to connect securely with the system, also ensuring long-term security of the protocol [3.5].

Finally, the Edinburgh research team explored the privacy limitations of traditional blockchain protocols. As the transaction ledger is a public resource, operational and transactional information may be leaked to an adversary. To address this problem in Ouroboros, the team introduced a new coin evolution technique relying on cryptographic primitives such as Succinct Arguments of Knowledge (SNARKs) and key-private forward secure encryption [3.6]. The resulting protocol, Ouroboros Crypsinous, became the first formally analysed privacy-preserving PoS protocol, further demonstrating the appeal to end-users.

The above results laid out a convincing pathway for the engineering of a full blockchain stack that is performant and energy efficient leading IOHK to adopt them as part of their development strategy for their main product, the Cardano blockchain.

3. References to the research

3.1. Kiayias A., Zhou HS., Zikas V. (2016) Fair and Robust Multi-party Computation Using a Global Transaction Ledger. In: Fischlin M., Coron JS. (eds) Advances in Cryptology – EUROCRYPT 2016. Lecture Notes in Computer Science, vol 9666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49896-5_25 **(100 citations; EUROCRYPT 2016 acceptance rate: 23%)**

3.2. Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In J. Katz, & H. Shacham (Eds.), *Advances in Cryptology -- CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20--24, 2017, Proceedings, Part I* (pp. 357-388). (Lecture Notes in Computer Science; Vol. 10401). Cham: Springer, Cham.

https://doi.org/10.1007/978-3-319-63688-7_12 **(792 citations, CRYPTO 2017 acceptance rate: 23%)**

3.3. David, B., Gaži, P., Kiayias, A., & Russell, A. (2018). Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Vol. 10821, pp. 66-98). (Lecture Notes in Computer Science (LNCS)). Springer. https://doi.org/10.1007/978-3-319-78375-8_3 **(181citations; EUROCRYPT 2018 acceptance rate: 24%)**

3.4. Gaži, P., Kiayias, A., & Russell, A. (2018). Stake-Bleeding Attacks on Proof-of-Stake Blockchains. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 85-92). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/CVCBT.2018.00015 **(64 citations)**

3.5. Badertscher, C., Gaži, P., Kiayias, A., Russell, A., & Zikas, V. (2018). Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 913-930). (CCS '18). New York, NY, USA: ACM. https://doi.org/10.1145/3243734.3243848 **(112 citations, CCS '18 acceptance rate: 18%)**

3.6. Kerber, T., Kiayias, A., Kohlweiss, M., & Zikas, V. (2019). Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake. In *Proceedings of the 40th IEEE Symposium on Security and Privacy 2019* (pp. 157-174). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/SP.2019.00063 **(22 citations; SP19 acceptance rate: 12%)**

Citation counts obtained from Google Scholar 2020-12-03.

Key research grants

European Commission: PANORAMIX (653497, GBP342,634); PRIViLEDGE (780477, GBP525,764)

4. Details of the impact

Input Output Hong Kong (IOHK) has called Ouroboros "the core component of Cardano", and its "backbone", asserting it "was very significant for its success." [5.1]

As a result of the research, IOHK was able to launch Cardano, a blockchain platform, along with the product Cardano ADA, a cryptocurrency that, thanks to the Ouroboros protocol, is ground-breaking in its security and energy efficiency. Ouroboros' proven impenetrability made it an extremely attractive protocol to underpin a financial system, which relies on trust and confidence to succeed. Bolstered by its energy efficiency – the only blockchain that provides such security for so little energy expenditure – this novel protocol has given IOHK a unique competitive advantage in the blockchain world, and has significantly contributed to both the innovation and the continued business success of the company.

Research conducted by UoE "significantly and fundamentally" benefitted IOHK, even prior to the development of Ouroboros [5.1]. Quoting research conducted by Kiayias at the University of Edinburgh (UoE) since 2015, IOHK confirms that the work conducted by UoE researchers on the Bitcoin protocol (e.g. 3.1) "provided concrete properties, blockchain protocol analysis techniques and a formal modelling framework that enabled the development of our software in a manner that minimized security vulnerabilities." [5.1] The company went on to hire Kiayias as their Chief Scientist in 2017, through a long-term consulting agreement between IOHK and the UoE [5.1].

Since 2015, IOHK has grown from a company of 2 to 200 team members worldwide [5.2, para. 19]. It credits the launch of Cardano in 2017 to its turnover of more than [text removed for publication] in contracts, representing an 11-fold increase in the value of the company [5.1]. The currency has attracted more than 80,000 users [5.1] and at its peak in 2018, its market capitalisation reached USD32,300,000,000 (01-2018), then representing 4.3% of the total market [5.3]. IOHK has also applied Ouroboros to a further product, its cryptocurrency wallet Daedalus, which leading cryptocurrency exchange platform Coinswitch describes as "safer than most because of the highly innovative and aggressive peer-research done regularly by its developers" [5.4]. Coinswitch has called Cardano ADA "the most advanced cryptocurrency in the world" [5.4].

DLT is increasingly being sought beyond the financial world as a measure to ensure fraud-proof record keeping in areas such as public service and local and national government. A 2016 report by the UK government's Chief Scientific Adviser stated:

> *Distributed ledger technologies (DLTs) have disruptive potential beyond innovation in products, services, revenue streams and operating systems within existing industry frameworks… Understanding this can help to frame the opportunities and threats afforded by distributed ledger technologies — and how they can inform changes in the role of the government, and the services it delivers.* [5.5, p. 53].

The report went onto cite the characteristics sought in a blockchain for such purposes as precisely those for which Ouroboros has been noted: "They need to be energy efficient….they should be highly resilient to attack." [5.5, pp. 11-12] In 2020, a Swiss draft law on the use of blockchain in civil law, insolvency law, financial market law, and banking law, explicitly cited Cardano as a "promising example" of DLT [5.6].

As well as attributing its financial success to Ouroboros, IOHK credits the research for its success in signing Memoranda of Understanding (MOU) with the governments of Georgia, Mongolia and Ethiopia [5.1]. The MOU have all been signed for the respective countries to form partnerships with IOHK, using Ouroboros's blockchain for public service systems of counterfeit detection and authentication. They demonstrate that impact surrounding the blockchain has been achieved at national policy level, and that movement is being made towards using the technology in civil service and international commerce in multiple parts of the world.

IOHK has stated: "We attribute the minimal energy expenditure allowed by Ouroboros to our success in securing government level interest in DLT, a million times better for the same level of decentralisation." [5.1]

The MOU signed by IOHK with the Ethiopian Ministry of Science and Technology concerns trialling DLT to authenticate Ethiopian coffee for export [5.7]; in Mongolia the MOU regards implementing blockchain to tackle counterfeit medicines [5.8]; and in Georgia, the technology is being used by the Ministry of Education, Science, Culture and Sports of Georgia for verifying education certificates in schools and universities [5.9].

In 2019 the Georgian Prime Minister's press office stated: "Work towards this end will be actively commencing from July 2019 and tangible results will be obtained by the end of the year." [5.10] Implementation of the project started in September 2019, and as of March 2020 the alpha version was already in use, with records in the process of being copied from their

existing server onto the blockchain [5.11]. Georgia is the first country to use a blockchain-based system in such a way, and IOHK is the first company to participate in a project of this nature.

The research has had significant impact in the innovation, rapid expansion and financial gain of IOHK and has led to pioneering changes in record keeping at national level, which continues to expand and progress.

5. Sources to corroborate the impact

5.1. Letter of corroboration from IOHK CEO

5.2. Kim, C. (2019, October 7). From Cardano to Ethereum, 2020 Could Be Deciding Year for Proof-of-Stake. Retrieved February 21, 2020, from https://www.coindesk.com/from-cardano-to-ethereum-2020-could-be-deciding-year-for-proof-of-stake

5.3. Cardano (ADA) price, charts, market cap, and other metrics. (2018). Retrieved August 18, 2020, from https://coinmarketcap.com/currencies/cardano/

5.4. Batabyal, A. (2020, May 6). Daedalus Wallet Review 2020 - Top 5 Pros and Cons. Retrieved August 15, 2020, from https://coinswitch.co/news/daedalus-wallet-review-2020-top-5-pros-and-cons

5.5. Walport, M. (2016, January 19) Distributed Ledger Technology: beyond block chain. Retrieved June 2, 2020, from https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

5.6. Brown, C. (2020, September 9). Switzerland: Draft law calls Cardano 'promising DLT'. Retrieved September 17, 2020, from https://www.crypto-news-flash.com/swiss-draft-law-refers-to-cardano-as-a-promising-dlt/

5.7. Castor, A. (2018, May 4). "Where Coffee Just Grows": Connecting Ethiopian Agritech to the Blockchain. Retrieved February 27, 2020, from https://bitcoinmagazine.com/articles/where-coffee-just-grows-connecting-ethiopian-agritech-blockchain

5.8. Teja, M. (2019, May 14). Cardano and Mongolian Government Signed an MoU to Fight the Counterfeit Drugs. Retrieved February 27, 2020, from https://crypto-daily.news/cardano-and-mongolian-government-signed-an-mou-to-fight-the-counterfeit-drugs/

5.9. Simmons, J. (2020, January 22). Cardano gains two new partners at the Davos World Economic Forum. Retrieved February 27, 2020, from https://www.crypto-news-flash.com/cardano-gains-two-new-partners-at-the-davos-world-economic-forum/

5.10. Georgian Prime Minister's Press Office. (2019, June 18). Blockchain Technology is to be Actively Introduced in Education Sector of Georgia. Retrieved October 28, 2020, from http://gov.ge/index.php?lang_id=ENG&sec_id=526&info_id=72356

5.11. Papidze, M. (2020, March 13) Georgia to be 1st country to put educational credentials on blockchain. Retrieved August 28, 2020 from https://agenda.ge/en/article/2020/12