Perspectives

Perspectives of Blockchain Technology, its Relation to the Cloud and its Potential Role in Computer Science Education

Ian Purdon
School of Computing
Eastern Institute of Technology
Napier, New Zealand
ipurdon@eit.ac.nz

Emre Erturk
School of Computing
Eastern Institute of Technology
Napier, New Zealand
eerturk@eit.ac.nz

***Abstract*— Blockchain ledgers and the Cloud are a perfect match. On the one hand, there is an inherent requirement for multiple separate authentication nodes to validate every Blockchain transaction with each node requiring substantial encryption calculation capability. On the other hand, massive economies of scale can bring down the cost per transaction, and provide service continuity. Additionally, the Cloud provides a perfect incubator for proof-of-concept projects. This paper considers the future implications of Blockchain, as the concept of disintermediated trustless ledgers stimulates the imagination of computer scientists and innovators. The Cloud's role in implementing this new paradigm is also highlighted, as a new decentralized P2P-Cloud model. Finally, this paper discusses how Blockchain may be integrated into the university level computer science and information technology curriculum.**

Keywords-Blockchain; Cloud; BaaS; IT Education

I. INTRODUCTION

Blockchain technology is defined as "a tamper-proof, shared digital ledger that records transactions in a public or private peer-to-peer network. Distributed to all member nodes in the network, the ledger permanently records, in blocks, the history of asset exchanges that take place …" [1]. Blockchain is named after its two key concepts: a) that all related simultaneous transactions are individually hashed and grouped into a "Block", which is cryptographically and uniquely identified with a Merkle root hash of all constituent hashes, and b) that each Block is permanently "Chained" to its immediate predecessor-Block. Integrity can be verified by using Merkle Proofs across the entire Blockchain, however Merkle branch, rather than the header's Merkle root [2]. The unique Blockchain contribution was to embed trust into the mechanism through two techniques, a) a free market of independent nodes where consensus of the majority verified integrity at every transaction, and b) permanent public visibility of the complete transaction chain via any of the distributed nodes [3]. For Bitcoin, the profit-motive ensures the multiplicity of independent nodes that is necessary for the integrity of a chain, but also that there is an inherent incentive and mechanism to fund the chain in-perpetuity. Blockchain implementations vary from the permission-less and completely decentralized model of Bitcoin, free of any restriction on participation other than compliance with its protocols, to hybrid permissioned architectures, where relationships and transactions are more formalized [4].

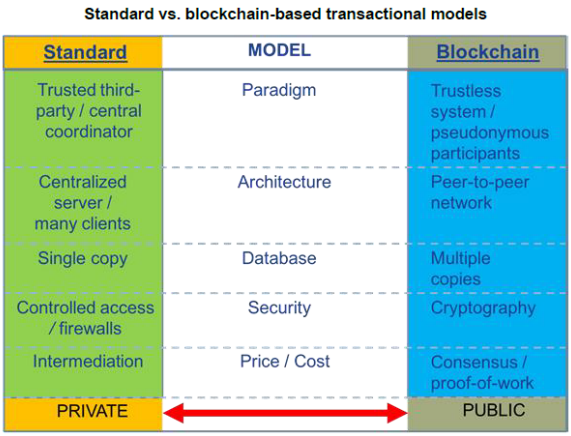

Fig. 1. The chracteristics of Blockchain technology, from [12]

Blockchain technology was developed initially for the Bitcoin cryptocurrency, to assure all parties that the payer had the means to satisfy the debt before concluding any transaction. However, much of the excitement (and hype) surrounding Bitcoin was really about recognizing the innovation of its 'trustless' decentralized and consensus-based architecture - this new paradigm had the potential to transform or disrupt many

industries, from keeping track of title-deeds for land-registries, to tracking diamonds, to resolving industry-wide legislative reporting requirements in the mineral extraction industry [5]. Within its first six years, Blockchain progressed from an idea, and simply being the Bitcoin enabler, to a "censorship-proof 'world computer'" [6]. In 2015, Melanie Swan noted the following categorizations of existing and potential uses [7]. Blockchain 1.0 corresponds to the original cryptocurrency uses. Blockchain 2.0 arrived with the launch of the Ethereum platform in January 2014, as an open-source platform enabling 'smart contracts', and focusing on financial contracts, loans, futures, stocks, etc. Blockchain 3.0 was defined to cover the gamut of all other non-financial usages, in government, health, science, art, and so on. As a result, Blockchain technology has already spawned a significant range of viable use-cases. Some authors see Blockchain as a foundational technology akin to TCP/IP, and predict an uptake and ubiquity of similar proportions: "It took more than 30 years for TCP/IP to move through all the phases: single use, localized use, substitution, and transformation, and reshape the economy… TCP/IP unlocked new economic value by dramatically lowering the cost of connections." Similarly, Blockchain also promises to dramatically reduce the cost of economic transactions. [8].

II. ROADBLOCKS AND EUPHORIA

Vitalik Buterin, internet prodigy and Chief Scientist at Ethereum noted that "Scalability is now at the forefront of the technical discussion in the cryptocurrency scene ...the Bitcoin network cannot process more than 7 transactions per second. If the popularity of Bitcoin jumps up tenfold yet again, then the limit will force the transaction fee up to nearly a dollar, making Bitcoin less useful than PayPal ... there is only really one optimization that can be made: figuring out some way to get past the obstacle that every full node must process every transaction" [2]. Bitcoin's need for transaction transparency as a means to establish trust is also a roadblock against greater penetration of the technology, as privacy and confidentiality are paramount for new users. Instruments with so-called Permissioned Blockchains are an attempt to limit and ensure secure access by only mutually known participants. The tendency to centralization due to the huge processing power required to verify transactions and mine new blocks is another major roadblock for conventional cryptocurrency Blockchain 1.0 implementation. Gartner Fellow and Vice President David Furlonger notes that Bitcoin "proof-of-work activity has been mostly consolidated into four primary mining organizations, all based in China". If collusion or a single organization can control 51% of the nodes, then the basis of distributed consensual trust is wholly negated. Additionally, consolidation of the IT sector, may mean that more and more Cloud-based solutions are being provided by the large corporations such as Amazon and Google. According to Kopstein, "a failure in one location potentially causes chaos for multiple companies and countless users" [9]. However, it is difficult not be engulfed in the wave of euphoria which underpins most Blockchain discussions. Melanie Swan, in her book 2015 'Blockchain: Blueprint for a New Economy', suggests that with its inherent decentralization, and as a new world-wide computing paradigm, it has "the potential for reconfiguring all human activity as pervasively as did the web … for the discovery, valuation, and transfer of all quanta (discrete units) of anything … hard assets … and intangible assets (votes, ideas, reputation, intention, health data)" [7]. Stephan Tual, CCO of Swiss non-profit startup Ethereum, claimed at their 2015 launch and 'smart contracts' Blockchain, that "The vision of a censorship-proof 'world computer' that anyone can program, paying exclusively for what they use and nothing more, is now a reality." He claims Ethereum as the "World's first zero infrastructure platform" [6]. In late 2016 Gartner had Blockchain close to arriving at the very pinnacle of their "Peak of Inflated Expectations", such is the fervor of its supporters [10]. Some of the reasons are elaborated on by Tyler Smith of BHP Billiton, in a speech to the International Blockchain Week 2016 conference organized by Consensys Media and ENS, where he espoused the virtues of a shared consortia model (group of like-minded but possibly economically competitive organizations) which would share and retain public information to meet the regulatory requirements of countries where they mine for resources, whilst saving both the host country and other industry participants billions of dollars which are currently wasted delivering an inferior library via inefficient systems [11].

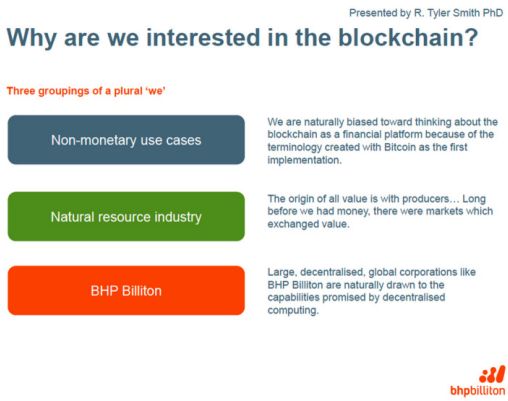

Fig. 2. Natural resources and mining industry's interest, fron [11]

The consortium model as proposed by BHP demonstrates the excitement surrounding Blockchain due to processing efficiencies, the imbued accuracy of original source transaction information sharing, and the increased integrity and provenance gained through the greater participation of sometimes competing member organisations.

III. BLOCKCHAIN AND THE CLOUD

The advantages of the Cloud were recognized very early in the commentary about Blockchain, especially as the world's major technology vendors exacerbate the hype by jostling for market-share, and attempting to leverage their existing investments in Cloud infrastructure. Ed Featherston writes in his blog, "public cloud providers have three key benefits to address the testing challenges: you can obtain your own dedicated testing environment... You only pay for what you use. You can configure for dynamic resource usage, allowing for true performance testing for application scaling and

identifying breakpoints" [13]. This essentially means a full blockchain ecosystem for users to start working with. From a user's perspective, the cloud seems to be at the heart of the birth of Blockchain, with the random democracy of Bitcoin node and mining participation fulfilling parts of the NIST definition of Cloud computing, as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" [14], or at least, helping define a new form of distributed Cloud termed P2P Cloud, best espoused by a company called STORJ, "the first decentralized, end-to-end encrypted cloud storage that uses blockchain technology and cryptography to secure your files." The article entitled 'Down with the data center: can a peer-to-peer swarm replace cloud computing?' argues that "we could wind up using P2P for some of the same tasks the cloud performs, with a distributed cloud instead of one focused around data centers, something less like a cloud and more like a swarm" [9]. The article goes on to illustrate this with startup Space Monkey putting a NAS into private homes, with a third of the capacity for personal use (with encrypted distribution protection), and the remainder for the P2P distributed data-center. The article also uses Bitcoin and Torrent as an argument for a new P2P data-sharing cloud paradigm.

The Cloud can mitigate many of the roadblocks previously noted for Blockchain, by providing BaaS, a ready-made ecosystem, with best-practice decentralization built into the service. In September 2016, a press release by IBM CEO states: "IBM Fuses Blockchain, AI and Cloud Computing into one unit" [15], which reinforces the intertwinement of Blockchain and the Cloud. As recently as January 2017, Microsoft trumpeted their Project Bletchley as the "code name for extending blockchain by creating both new middleware as well as secure cryptlets", offering Blockchain as a Service (BaaS) on their Azure Cloud. Froystad further elaborates on the Ethereum / Microsoft liaison: "What Ethereum has gained through this partnership, is not only legitimacy but also a world-wide network of data centers that makes it significantly easier to launch a blockchain application. Azure is available in 24 regions around the world, so that anyone anywhere can spin up a private blockchain" [16]. This is a way to fail fast and cheap at blockchain projects, and then figure out better ways to use the technology. This is a worldwide distributed lab environment for banks and consortia. By partnering with a company called Ripple, whose specialty is inter-ledger protocols, Microsoft has further leveraged itself as platform-neutral in the cloud delivery of Blockchain services.

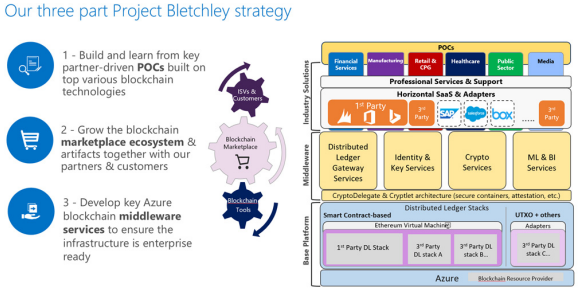

Fig. 3. Microsoft's Blockchain Project [17]

IBM have partnered with the Linux Foundation's Hyperledger offering, leveraging their BlueMix Cloud and LinuxONE cloud-capable mainframes. A good example of practical success is Everledger, a startup guaranteeing provenance of individual diamonds traded around the world, by recording unique aspects of each stone, like a fingerprint, which then uses Hyperledger.org's open-source Blockchain in the Cloud hosted by The Linux Foundation, to record every transaction, with so much success that insurance companies can now repatriate assets, and identify 'blood diamonds' [18]. The Linux and Blockchain connection is also an interesting aspect by itself, and attests a new area where open-source technology can be globally beneficial [19]. Amazon are using AWS for their foray into financial Blockchain use, announcing a "BaaS sandbox for developers" in partnership with Digital Currency Group, "to spur innovation and facilitate frictionless experimentation" [20], as reported by Richard Kastelein, which also quotes DCG's Director of Community, Meltem Demirors as saying "the venture capital model has to evolve to enable disruption in financial services, and AWS was a natural collaborator given most of our portfolio relies on the AWS Cloud.". There are advantages to using the Cloud to host blockchains. Cloud service providers are offering template driven trials, with very low cost of entry via BaaS provisioning, and pay-as-you-go operation. This involves user selectable number of nodes, and the inherent advantages of scalability.

Vendor organizations, with existing Cloud services, are actively seeking industry partnerships and proof-of-concept projects in order to position themselves as major Blockchain innovators, often providing free Starter Plans. In Permissioned Blockchains, a consortium of like-minded participants each contribute their own node as part of a pan-industry Blockchain initiative. Nodes could be provisioned privately, or use hybrid cloud infrastructure. Google's subsidiary DeepMind Health's project for managing and protecting the UK's health data uses a Blockchain-like strategy to assure the public of its purely-intentioned analytical access to otherwise confidential personal health records [21], however in this particular implementation "the ledger won't be distributed among members of the public, but stored by a number of entities including data processors like DeepMind Health and health care providers." According to the company, this will not impede the verification process. The objective of this choice is to make the ledger more efficient.

IV. THE FUTURE OF BLOCKCHAIN IN THE CLOUD

While permissioned private consortia will always make up a significant segment of Blockchain implementations, the larger potential appears to be in non-partisan sector-wide implementations, leveraging the value of separate nodes and invoking economies of scale from Cloud infrastructure, to yield efficiencies through the strength of the architecture and the value of the shared data. While outlining the implications of new European Union rules governing the finance and investment sector, i.e. MiFidII (Markets in Financial Instruments Directive) due to come into force in January 2018, Noelle Acheson writes that Luxembourg's Fundchain Consortium is attempting "a sector-wide system that can leverage transparency, reliability and connectivity. Plus, a way to share pricing and identity data without the risk of

interference or centralized control" [22]. She goes on to say that "If Luxembourg's fund managers, service providers and regulators manage to adapt and implement a new type of interaction, the sector could be poised to harness the financial trends that point to an even greater role for wealth management in the world economy.". Outside of major institutions who may form such a consortium, and who have the capacity to maintain their own nodes privately, the vast majority of lesser solutions are likely to be built on platforms provided by the industry's heavy-hitters, and especially those that have claimed the altruistic high-ground, as Ethereum has done as a non-profit organization. Similarly, Chronicled.com aims at providing a Blockchain platform "To create the world's most trusted IoT and supply chain ecosystems", using Quorum, Hyperledger, or Ethereum's Cloud offerings." . It is likely that the near future will see a plethora of infrastructure and vendor offerings, and a multitude of proof-of-concept and operational systems, which may converge, as Blockchain matures along with growing confidence. Microsoft noted in reference to Project Bletchley, that "creating this open ecosystem will take some time. But if done properly the combination of distributed ledgers and the Cloud can usher in the new collaborative economy" [23]. BHP Billiton's geophysicist R Tyler Smith explains their P2P infrastructure as follows: "In addition working with Ethereum, BHP is also running its own nodes on the InterPlanetary File System (IPFS), a peer-to-peer file sharing protocol that is increasingly being used in conjunction with blockchain systems" [5]. As Kopstein noted, there could also be a divergence from the traditional datacenter Cloud infrastructure, towards a truer distributed and unrelated Peer to Peer Cloud infrastructure, which would add further integrity and stability to Blockchain implementations, with true disintermediation from any single party [9].

V. SUMMARY AND CONCLUSION

Integrity in a Blockchain is guaranteed because previous data cannot be modified, each block cryptographically references the immediately prior block, and all nodes maintain a complete transcript. The immutability and the continual need to re-assert the full chain at every transaction may become an issue in the future unless ways are developed to streamline it. While data scientists continue to grapple with the issue of scalability, and organizations feel their way through the hype, it is worth noting how far the idea has come in a few years, and the range of industries attempting to realize its potential, from the original cryptocurrencies and financial securities to property registries and diamond and art provenance. Furthermore, many of the software processes related to blockchains can be executed by so-called Intelligent Agents that can work and develop flexibly and independently [24]. Concomitant with Bitcoin and Blockchain, the Cloud has been an incubator, both through major IT vendors jostling for market-share, but also by provisioning Blockchain as a Service on their Cloud infrastructure. This fortuitous circumstance facilitates proof-of-concept applications without requiring significant startup costs or long-term commitment. Using an innovative technology particularly suits online education providers or providers that are designing a new information system [26]. In this context, the hosting of software in the Cloud also enables end users to connect and perform searches and queries through their mobile devices. Blockchain technology has started being used in the education sector. One example of this is the issuance, tracking, and verification of certificates through a blockchain database, which is used either by a single institution or a consortium of education institutions [27].

Furthermore, coupling a blockchain application with cloud use cam also facilitate the demonstration, use, and learning of this new technology at universities and other technology training situations. On one hand, the topic of Blockchain may not take off initially and be as popular as Internet of Things (IoT); since the latter also appeals to primarily kinetic and active learners, for example, through the use of connected robots and kits. There are also more job openings that are related to IoT, as opposed to jobs involving blockchains. Another concern will be around where to place and teach this concept in the computer science and information technology curriculum. The general options for covering any advanced topic include: placement within existing courses (generally at higher or graduate levels), creating new courses for the topic or technology, and addressing the new technology through extra-curricular activities such as a symposium, guest speaker, or campus club [25]. The first one of the options above, using Blockchain as a novel example or sub-topic within existing courses, has appeal, because it can help make the course more fun and interesting, in addition to being very feasible. This may be in the form of a theoretical discussion as well as a hands-on application. Possible computer science courses that may incorporate a blockchain application include database systems, cloud computing, computer networking, advanced business information systems, computer security, computer cryptography, web hosting, and web administration. The authors of this paper hold the position that more research and preparation will be worthwhile to incorporate this interesting topic into the curriculum. Teaching a blockchain application will be easier in the Cloud, without needing or dedicating additional local hardware. Therefore, a good follow-up project is to demonstrate step-by-step in detail how to host, run, and maintain a blockchain application using one of the popular cloud platforms available to university and tertiary institutions such as the Google Compute Engine, Amazon AWS, or Microsoft Azure.

REFERENCES

[1] S. Brakeville, B. Perepa, "Blockchain Basics: Introduction to Distributed Ledgers", https://tinyurl.com/ya6g6v2w

[2] E. Buterin, "Ethereum Scalability and Decentralization Updates", https://tinyurl.com/y83q53h9

[3] P. Evans, "A Strategic Perspective on Blockchain and Digital Tokens", https:// tinyurl.com/hqldvyq

[4] M. Herlihy, M. Moir, "Enhancing accountability and trust in distributed ledgers", https://arxiv.org/pdf/1606.07490.pdf

[5] P. Rizzo, "World's Largest Mining Company to Use Blockchain for Supply Chain", https://tinyurl.com/y85eh24t

[6] S. Tual, "Annoncement: Ethereum Launches", https://tinyurl.com/paqpppp

[7] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015

[8] M. Lansiti, K. R. Lakhani, "The Truth about Blockchain", Harvard Business Review, pp. 118-127, January/February 2017.

[9] J. Kopstein, "Down with the Data Center", https://tinyurl.com/y7dme9dp

[10] A. Forni, R. Meulen, "Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage", https://tinyurl.com/zh4n83z

[11] G. Samman, "Consortiums and Shared Ledgers: Supply Chains as a Use Case", https://tinyurl.com/ycr8hqlo

[12] A. Collomb, K. Sok, "Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector?", DigiWorld Economic Journal, Issue 103, 2016

[13] E. Featherston, "Moving Test Environments to the Cloud", https://tinyurl.com/ycbuptfd

[14] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", https://tinyurl.com/zjqy993

[15] R. Kastelein, "IBM Fuses Blockchain, AI and Cloud Computing into One Unit", https://tinyurl.com/ybkp85w2

[16] P. Froystad, "Analysing the Ethereum/Microsoft BaaS Solution", https://tinyurl.com/ydhk3jal

[17] W. Spies, "Blockchain Basics and Partner Strategy", https://tinyurl.com/y6ugr8gw

[18] H. Levy, "The CIO's Guide to Blockchain", https://tinyurl.com/h6ewetb

[19] E. Erturk, "International technology transfer: the case of free computer software", International Academy of Business and Public Administration Disciplines (IABPAD) Conference, Orlando, Florida, 2009.

[20] R. Kastelein, "Amazon Announces Blockchain-as-a-Service (BAAS) Sandbox for Developers", https://tinyurl.com/y8psk9yc

[21] J. Vincent, "Google's AI Subsidiary Turns to Blockchain Technology to Track UK Health Data", https://tinyurl.com/y8adefet

[22] N. Acheson, "Why a Quiet Blockchain Consortium Could Soon Make Noise", https://tinyurl.com/ld66hlr

[23] M. Gray, "Introducing Project Bletchley", https://tinyurl.com/j9lhee5

[24] M. Odhiambo, P. Umenne, "NET-COMPUTER: Internet Computer Architecture and its Application in E-Commerce", Engineering, Technology & Applied Science Research, Vol. 2, No. 6, pp. 302-309, 2012

[25] S. Kursh, N. Gold, "Adding Fintech and Blockchain to Your Curriculum", Business Education Innovation Journal, Vol. 8, No. 2, 2017

[26] E. Erturk, "An Intelligent and Object-oriented Blueprint for a Mobile Learning Institute Information System", International Journal for Infonomics, Vol. 6, No. 3/4, 2013

[27] D. Clark, "10 Ways Blockchain Could Be Used in Education", https://tinyurl.com/ycd3uxtg

AUTHORS PROFILE

Ian Purdon is a lecturer and postgraduate student at the Eastern Insittute of Technology in New Zealand. He is enthusiastic about computers. Ian is also the former IT Development Manager of ENZAFOODS NZ Limited.

Emre Erturk received his Ph.D. from the University of Oklahoma in 2007. He has later taught as an Adjunct Associate Professor with the University of Maryland (USA). Currently, he works at the Eastern Institute of Technology, New Zealand. He has been involved in many IT conferences and publications around the world.