Blockchain beyond Bitcoin

By Ghassan Karame and Wenting Li

The notion of blockchain traces back to the Bitcoin protocol [1], which is a digital currency that acquired considerable popularity since its launch in 2009. Bitcoin builds a payment service on top of an underlying peer-to-peer network which ensures that all transactions and their order of execution are available to all users of the system.

To this end, Bitcoin relies on a Proof-of-Work (PoW) scheme that allows users to "mine" for digital coins (BTCs) by performing computations. More specifically, to generate a block, Bitcoin peers must find a nonce value that, when hashed with additional fields (i.e., the Merkle hash of all valid and received transactions, the hash of the previous block, and a timestamp), the result is below a given target value. If such a nonce is found, peers then include it (as well as the additional fields) in a block thus allowing any entity to publicly verify the PoW. Upon successfully generating a block, a peer is typically granted a number of new BTCs. This provides an incentive for peers to continuously support Bitcoin. The resulting block is forwarded to all users in the network, who can then check its correctness by verifying the hash computation. If the block is deemed to be "valid", then the users append it to their previously accepted blocks, thus growing the Bitcoin block chain. Bitcoin relies on this mechanism to resist double-spending attacks; for malicious users to double-spend a BTC without being detected, they would not only have to redo all the work required to compute the block where that BTC was spent, but also they need to recompute all the subsequent blocks in the chain.

The security and privacy of the system were at the core focus of the research community. The work of Karame et el. [2] thoroughly explored the double-spending issue in Bitcoin network; the authors showed that the double-spending attacks can be achieved with high probability when used in fast payment scenarios (i.e., when the merchants do not wait until the transaction is confirmed by the network). The privacy and anonymity provisions of Bitcoin were also investigated in [3] [4] [5]; these studies have shown that Bitcoin leaks considerable information about its users since all transactions (including the timing and amounts exchanged) are public.

This motivated considerable research to enhance the security and privacy of the system, e.g., Mixcoin [6], CoinJoin [7], Zerocoin [8] and Liquid [9]. For instance, Liquid is a sidechain of Bitcoin contributed by the Elements project [10]. This project aims to combine different composable security features such as confidential transactions and segregated witnesses to enhance the security and privacy of the system. On the one hand, confidential transactions improve the privacy by hiding the transaction amounts using homomorphic additive encryption, while allowing the public network to validate if the transaction entries add up correctly. On the other hand, segregated witnesses prevent the malleability attacks by splitting the validation component apart from the transaction payloads.

In the last couple of years, research unveiled an overlooked potential and a truly genuine breakthrough within Bitcoin, the *blockchain*. The blockchain emerges as a novel distributed consensus scheme which allows transactions, and any other data, to be securely stored and verified without any centralized authority. Notice that the entire community has been in search for a simple and workable distributed

consensus protocol for a considerable amount of time. The well-known "Paxos" algorithm is complex enough and does not meet the need of our applications. Recently, Stanford engineers published a paper entitled "In Search Of An Understandable Consensus Algorithm" which shows the need of an efficient distributed consensus algorithm.

As such, Bitcoin's blockchain fueled innovation, and a number of innovative applications have already been devised by exploiting the secure and distributed provisions of the underlying blockchain. One of the most prominent examples of the application of the blockchain is Namecoin. Currently, ICANN centrally governs nearly all top-level Web address domains such as ".com." Namecoin serves as a new domain-name system for registering Web addresses that end in ".bit." In this case, instead of ICANN controlling the domain name system, participants in the Namecoin system control the domain names.

Other prominent applications include secure timestamping [11], secure commitment schemes [12], secure multi-party computation [13] [14], and smart contracts. Notice that some of these extensions cannot be deployed without changing the code base of Bitcoin (i.e., via a hard fork). These are referred to as altcoins and require some measures to initiate currency allocation (e.g., via pegged sidechains [15]) and preserve mining power (e.g., via merged mining [16]) by leveraging the already established Bitcoin community. Recently, IBM proposed the notion of Device Democracy [17], with the goal to support consensus across a fully meshed network of IoT devices based on the blockchain technology.

Other blockchain technologies were also proposed almost independently from Bitcoin. Many of those propose to replace Bitcoin's proof-of-work in order to cater for its energy waste and scalability limits. For instance, a number of contributions propose the reliance on memory-based consensus protocols [18] or virtual mining such as proof-of-stake [19] [20]. Other proposals [21] [22] [23] resort to the classic Byzantine fault tolerant consensus protocols in the hope to increase the ledger closure efficiency and achieve high transactional throughputs. Moreover, in contrast to the UTXO (Unspent Transaction Output) model used in Bitcoin and its altcoins, some blockchains adopt models such as credit networks [24], or account-based model in which transactions directly link to the issuer accounts instead of pointing to the output of previous transactions [25].

Among these alternative blockchains, Ripple, the current holder of the second largest market capitalization after Bitcoin, maintains a distributed ledger which keeps track of all the exchanged transactions and account states in the system. Ledgers are created every few seconds, and contain a list of transactions to which the majority of validating servers have agreed to. This is achieved by means of Ripple's proprietary consensus protocol [21] which is an iterative process and is executed amongst validating servers. Ripple has its own currency called XRP; it also accepts credit-based payments (I Owe You transaction model) if a trust path between the sender and receiver exists. Ripple has been recently criticized for its centralized deployment (as most of the validation nodes are maintained by Ripple Labs); the underlying consensus protocol of Ripple has also received considerable criticism [26]. Stellar [27] shares a similar model as Ripple, but relies on a federated Byzantine agreement protocol in order to resolve the various issues faced by Ripple.

Ethereum [28] brings a new dimension to the blockchain, as it expands the standard application of blockchains from the mere public bulletin board approach to a general-purpose peer-to-peer

decentralized platform for executing smart contracts. Namely, Ethereum enables any entity to create and deploy novel applications by writing decentralized contracts. The contract itself is a small program which maintains its own key-value store through transaction calls. Therefore, multiple application services can run on the shared Ethereum platform, whose role is to maintain consensus in the network. The current consensus protocol used in Ethereum is GHOST [29], which is a variant of proof-of-work. The next generation of Ethereum, however, is expected to adopt a more efficient security-deposit proof-of-stake consensus protocol [30].

IBM's OpenBlockchain (OBC) [31] is mainly inspired by Ethereum and equally provides a general-purpose application platform. In addition, OBC introduces membership services to provide authorization for participation, and offers confidentiality for transactions.

Nevertheless, in spite of considerable research in this area, there are still many challenges that need to be overcome, namely:

1. *Scalability*: Existing blockchain technologies (based on BFT or PoW consensus protocols) cannot match the transactional volume of Visa (47,000 transactions per second). There are currently several attempts to devise new blockchain platforms that can effectively scale to a large number of participants without compromising the attained transactional throughput.
2. *Limits of (De-)centralization*: One of the main attractions of the blockchain lies in its decentralized aspects. Although most blockchains are designed for full de-centralization, recent studies showed the limits of decentralization in their current deployment, as several essential services built around the blockchain cannot be effectively de-centralized [13].

Bibliography

[1] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: http://www.bitcoin.org/ bitcoin.pdf.

[2] G. Karame, E. Androulaki and S. Capkun, "Double-Spending Attacks on Fast Payments in Bitcoin," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, USA, 2012.

[3] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating user privacy in bitcoin," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, Okinawa, Japan, 2013.

[4] A. Gervais, V. Capkun, S. Capku and G. O. Karame, "Is Bitcoin a decentralized currency?," in *IEEE Security and Privacy*, 2014.

[5] A. Gervais, G. O. Karame, D. Gruber and S. Capkun, "On the Privacy Provisions of Bloom Filters in

Lightweight Bitcoin Clients," in *Proceedings of the 30th Annual Computer Security Applications Conference (ACM ACSAC)*, New Orleans, Louisiana, USA, 2014.

[6] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll and E. W. Felten, "Mixcoin: Anonymity for Bitcoin with accountable mixes," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, 2014.

[7] G. Maxwell, "CoinJoin: Bitcoin privacy for the real world," 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=279249.0.

[8] I. Miers, C. Garman, M. Green and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *2013 IEEE Symposium on Security and Privacy*, 2013.

[9] "Sidechain Liquid," [Online]. Available: https://elementsproject.org/sidechains/liquid/.

[10] "The Elements Project," [Online]. Available: https://elementsproject.org/.

[11] G. Bela, N. Meuschke and A. Gernandt, "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin," rXiv preprint arXiv:1502.04015, 2015.

[12] J. Clark and A. Essex, "Commitcoin: Carbon dating commitments with bitcoin.," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, 2012.

[13] M. Andrychowicz, S. Dziembowskil and D. Malinowski, "Secure multiparty computations on bitcoin," in *2014 IEEE Symposium on Security and Privacy (SP)*, 2014.

[14] G. Zyskind, O. Nathan and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," 2015. [Online]. Available: http://enigma.mit.edu/enigma_full.pdf.

[15] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón and P. Wuille, "Enabling blockchain innovations with pegged sidechains," 2014. [Online]. Available: http://cryptolibrary.org/bitstream/handle/21/406/2014_Back_Enabling_blockchain_innovations_with_pegged_sidechains.pdf?sequence=1.

[16] "Bitcoin Wiki - Merged Mining," [Online]. Available: https://en.bitcoin.it/wiki/Merged_mining_specification.

[17] "Device Democracy Whitepaper," [Online]. Available: http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/.

[18] G. Ateniese, I. Bonacina, A. Faonio and N. Galesi, "Proofs of space: When space is of the essence," in *Security and Cryptography for Networks*, 2014.

[19] V. Buterin, "Slasher: A punitive proof-of-stake algorithm," 2014. [Online]. Available: https://blog.ethereum. org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm.

[20] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," 2012. [Online].

Available: http://wallet.peercoin.net/assets/paper/peercoin-paper.pdf.

[21] D. Schwartz, N. Youngs and A. Britto, "The Ripple protocol consensus algorithm," 2014. [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[22] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," 2015. [Online]. Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[23] "IBM OpenBlockChain," [Online]. Available: http://www.ibm.com/blockchain/.

[24] "Ripple Wiki - Payment IOUs," [Online]. Available: https://wiki.ripple.com/Payments#IOUs.

[25] "Ethereum Whitepaper," [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[26] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef and E. Zenner, "Ripple: Overview and Outlook," in *Proceedings of International Conference on Trust and Trustworthy Computing*, Crete, Greece, 2015.

[27] "Stellar," [Online]. Available: https://www.stellar.org/.

[28] "Ethereum Project," [Online]. Available: https://www.ethereum.org/.

[29] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains," IACR Cryptology ePrint Archive 2013, 2013.

[30] V. Zamfir, "Introducing Casper "the Friendly Ghost"," [Online]. Available: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.

[31] GitHub, "OpenBlockChain Whitepaper," [Online]. Available: https://github.com/openblockchain/obc-docs/blob/master/whitepaper.md.

[32] "NameCoin," [Online]. Available: https://namecoin.info/.

[33] "Bitcoin Wiki - Contract," [Online]. Available: https://en.bitcoin.it/wiki/Contract.

[34] Linux Foundation, "Hyperledger Project," [Online]. Available: https://www.hyperledger.org/.

[35] M. Vukolic, "The Quest for Scalable Blockchain Fabric : Proof-of-Work vs . BFT Replication.," 2015. [Online]. Available: http://www.vukolic.com/iNetSec_2015.pdf.