Marta Misiaszek - Schreyner
Mirek Sopek

CKA as a tool for blockchain technology

April 4, 2022

1 Blockchain technology

A blockchain is an architecture that enables data to be stored in a decentralized network [1]. The main difference between an traditional database and blockchain is that it allows information to be linked by blocks rather than by relation of the raw data elements. Each block in a blockchain contains some data, the hash of the block itself, and the hash of the previous block. The data stored inside a block depends on the type of blockchain (for example, the Bitcoin blockchain stores transaction details, such as the sender, receiver, and number of coins). Each block also has a hash, which is a fingerprint that identifies the block. It is always unique, calculated once a block is created. Thus, any change inside the block will cause the hash to change. The hash of the previous block contained inside each block allows for creating the ledger or a chain of blocks.
Blockchain blocks need not necessarily be in the form of uniform binary data blocks. Modern solutions allow for much richer data structures to be linked [2] to form the chain. What is essential is that the entire system represents a consistent generalized transaction history on which all nodes achieve eventual agreement about the linked data.

The main components of blockchain software are consensus and validation algorithms that provide transparency and data security. Unlike ordinary databases, a public blockchain does not rely on centralized model of trust because it is fully available for anyone that wants to participate as a node. Such node gets a full copy of the blockchain and can even use the copy of the blockchain to verify that everything is in order. Therefore the security of a blockchain comes not only from the creative use of encryption, hashing and consensus mechanisms, but also from being distributed and decentralized.

Despite the common features of the blockchain software, there are various consensus mechanisms, for example: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA), Proof of Capacity (PoC) and many others [3]. All of them are the mathematical

operations through which nodes from the network validate creation of new blocks, however, they differ in the type of algorithm that is used. The most popular and most famous is PoW (used in Bitcoin, early Ethereum and other networks), despite the fact that it needs high computational effort that results in high energy consumption.

Regardless of the many advantages of the blockchain, there are huge drawbacks that outcomes from its distributed architecture. In theoretical considerations of distributed systems there are two fundamental theorems that limit desirable properties of blockchain architecture. One of them is known as **CAP theorem** [4], the other is **FLP impossibility result** [5].

CAP theorem [4] states any distributed system can have at most two of the following three properties:

- → consistency (C) – every read receives the most recent write;
- → availability (A) – each request eventually receive a response;
- → partition tolerance (P) – the system operates despite an arbitrary number of messages being dropped between nodes due to communication breakdowns or any other reasons.

Unfortunately, the CAP theorem oversimplify the balance between these properties. Due to that this formulation is not genuinely true. CAP theorem states only that perfect availability and consistency in the presence of partitions is not possible. Therefore the designers of distributed systems does not need to choose between consistency and availability when partitions are present. The goal is rather to find a trade-off between them.

The FLP impossibility result [5], named after its authors (Fischer, Lynch and Patterson), comes from consideration on achieving consensus in distributed systems. It shows that in an asynchronous setting, there is no distributed algorithm that always solves the consensus problem, even if only one node of the system is fault.

The limits ensuing from both CAP and FLP theorems translate to the phenomenon called the **blockchain trilemma**: *it is impossible for any classical blockchain to simultaneously guarantee security, scalability and decentralization*. Various blockchain consensus algorithms attempted to find a balance between these three features, resembling the trade-offs made by the designers of standard distributed systems. One of the approaches to minimize the negative effects of the trilemma is to prioritize data availability (i.e. scalability) and agree that the data may not be consistent on all nodes at the same time, but to demand that it is eventually consistent, i.e. after some time of the system life.

Since these problems are crucial for the blockchain technology, it is important to analyse new proposals and test new algorithms. Luckily, recent works [6] shows that the use of quantum mechanical laws and mechanisms can be beneficial for reduction of negative consequence of the trilemma and could lead to entirely new class of blockchain architectures.

However, at the same time the emerging quantum computers pose a threat to the security of modern blockchains, which are built mostly as P2P networks and assume heavy use of the classical asymmetric cryptography with public-private keys playing a pivotal role. Therefore, it is wise to explore the possibilities of integration of quantum cryptography and quantum devices in the blockchain architecture.

Quantum secured blockchain

As it was mentioned earlier, the quantum computers pose a threat to any classical encryption algorithms that are used nowadays. Therefore, blockchain protection with quantum cryptography is a sensible step in further development of this technology.

This development may take many different paths.

- → One is to use simply the quantum random number generator for creating the encryption keys. Since such keys have higher degree of randomness than generated using any available algorithms, or obtained using any classical physical processes, this way of communication is a way more secure than the communication that is currently provided.
- → The second is the use of quantum key distribution (QKD) devices that are available on the market and setting quantum channels between each node of the blockchain network (one to one architecture). The use of these devices for obtaining consensus significantly increases the security and ensures the validity of a newly created blocks. Also, as shown in Ref. [7], another type of consensus mechanism can be used, which, by using one-time pad encryption keys further improves the security of the blockchain.
- → The third method is to explore different quantum communication protocols that enable the use of other network architectures and favorably affect scalability of such network.

The third development path offers the novelty the most therefore, in particular, it is elaborated further in this work.

2 Quantum Key Distribution

Similarly to classical way of data encryption, quantum cryptography also bases on key distribution. The difference here is that the key is generated by non-deterministic purely random process. This process, which occurs in consistence with quantum mechanical laws, secures the distribution of a key itself. For example, since quantum state collapses when measured, the eavesdropping of transmission can be easily detected. Also, due to no-cloning theorem [8], it is impossible to copy the data that is encoded in a quantum state. All of this makes quantum key distribution (QKD) *an*

information-theoretically secure solution to the key exchange problem.

There are many protocols used for QKD. One of the best known is BB84 [9], named after Charles Bennett and Gilles Brassard whose presented it in 1984. In this protocol secret key is encoded in photons' polarization states, randomly chosen from two available basis. Each photon represents a single bit of data. Its value is established after the transmission of a photon through the quantum channel and the measurement of its polarization state. Since the measurement is done in two basis, that are also randomly chosen, the outcome of the measurements need to be reconciled by communicating parties. It is done through classical channel (such as phone, mail or any other similar way of communication). Unfortunately, due to that, in the worst case, half of sent bits may need to be removed from the key. Moreover there are also other losses, decoherence and measurement imperfections that may influence the rate of established key.
Furthermore, the standard QKD protocols such as that presented above requires to set the quantum channels between all communicating parties. It means that for N parties it is needed to have $\frac{N(N-1)}{2}$ connections.

All of this, combined with the high cost of available QKD systems, results in slowdown in development of the commercial use-cases of quantum cryptography.

Fortunately, there is novel QKD protocol that allows to decrease the number of connections in the system to N for N communicating parties. It is called Quantum Conference Key Agreement (CKA).

Quantum Conference Key Agreement

Quantum Conference Key Agreement is a protocol that enables the multi-party quantum key exchange [10]. It means that the same quantum key is established between many parties. As it is elaborated further, thanks to that it is possible to achieve consensus in a multiparty system.

CKA is based on sharing N qubits with N communicating parties. These qubits are in specific entangled state called $|GHZ\rangle$.

The CKA protocol was experimentally demonstrated in a scheme with 4 node network in 2021 [11]. The experimental setup is presented in Figure 1.
As it can be seen, the nodes are connected in both ways, with quantum channels to the quantum server, and with each other by classical channel. The quantum server is responsible for distribution of an entangled state, which is here in a form

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\Big(|0000\rangle + |1111\rangle\Big) .$$

Such quantum state is generated using two SPDC sources in Sagnac mode (here PPLN crystals), pomped by pulsed Ti:Sapphire laser, and distributed using long single-mode fibers. Then, each node measures its qubit similarly

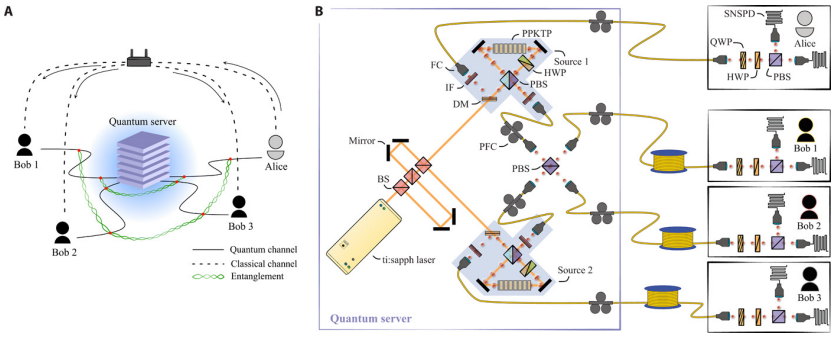

Figure 1: Depiction of CKA for 4-node network. The figure is taken from Ref. [11]. A) The idea of the network with a quantum server. B) Experimental setup.

to the method used for standard BB84 protocol (collecting detections for different settings of quarter and half waveplates).

Although the experimental realization was presented only for 4 nodes separated from each other by 20 km at maximum, due to the scalability if this method, it is a promising solution worth to consider in further development of quantum consensus mechanism in distributed systems.

3 Quantum distributed consensus algorithm and FLP impossibility

As it was mentioned earlier, the **GHZ state** is one of the quantum mechanical tools that enables to achieve distributed consensus [6, 12]. In general, GHZ state is an ensemble of N entangled qubits, which state may be mathematically written as

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes \mathrm{N}} + |1\rangle^{\otimes \mathrm{N}}\right).$$

Similarly to the experiment present in previous section, each node in a network receives a single qubit and measures it, choosing "0" if measured state is $|0\rangle$ and 1 otherwise. Due to that the single measurement causes collapse of qubit state to $|0\rangle$ or $|1\rangle$ for each participant of communication, not only those who made the measurement, this allows for obtaining a consensus on single bit of information between multiple nodes.

Such method provides all properties of distributed consensus [3, 5]:

- → agreement – provided by quantum mechanics (measurement of any entangled qubit cause all other qubits to collapse into an identical state);
- → validity – provided by proposing either "0" or "1" after the measurement done by first node;

→ wait-free processing – provided by the entanglement, i.e. the quantum state of all qubits collapses simultaneously.

It is worth to mention that faulty nodes do not influence achievement of the consensus, because the consensus is obtained after any measurement performed by any node.

Summarizing, the use of GHZ state enables to achieve the consensus in distributed systems and, what is more, overcome FLP impossibility result.

4 Further work

All information above provide a conclusion that development of blockchain technology should take benefits from the law of quantum mechanics. Therefore it is important to not only switch the type of communication between classical and quantum one, but also to investigate novel models of consensus algorithms, reflecting, among other challenges the topologies and architectures of the quantum networks.
For this reason, despite the fact it needs some amendments for the use in commercial products, CKA protocol may be interesting solution to the consensus problem in distributed systems. Especially, as shown above, if it solves the FLP impossibility result problem.

5 Bibliography

[1] R. Wattenhofer, *Distributed Ledger Technology. The Science of the Blockchain*, Createspace Independent Publishing Platform, revised 2017.

[2] M. Sopek, D. Tomaszuk, Sz. Głąb, F. Turoboś, I. Zieliński, D. Kuziński, R. Olejnik, P. Łuniewski and P. Grądzki, *Technological Foundations of Ontological Ecosystems on the 3rd Generation Blockchains*, IEEE Access, vol. 10, pp. 12487-12502, 2022, doi:10.1109/ACCESS.2022.3141014.

[3] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, L. He, *A Comparative Study of Blockchain Consensus Algorithms*, J. Phys.: Conf. Ser. **1437**, 012007 (2020).

[4] S. Gilbert, N.A. Lynch, *Perspectives on the CAP Theorem*, Computer **45**(2), 30 (2012).

[5] M.J. Fischer, N.A. Lynch, M.S. Paterson, *Impossibility of Distributed Consensus with One Faulty Process*, Journal of the ACM **32**(2), 374 (1985).

[6] M. Marcozzi, L. Mostarda, *Quantum Consensus: an overview*, arXiv: 2101.04192 (2021).

[7] X. Sun, M. Sopek, P. Kulicki, *Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic*, Entropy **21**(9), 887 (2019).

[8] W. Wootters, W. Zurek, *A Single Quantum Cannot be Cloned*, Nature **299**(5886), 802 (1982).

[9] C.H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing **175**, 8 (1984).

[10] F. Grasselli, *Quantum Cryptography: from Key Distribution to Conference Key Agreement*, PhD thesis from the Institute for Theoretical Physics III at the Heinrich-Heine-Universität Düsseldorf (2020).

[11] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, A. Fedrizzi, *Experimental quantum conference key agreement*, Sci. Adv. **7**, 23 (2021).

[12] E. D'Hondt, P. Pamamgaden, *The Computational Power of the W and GHZ states*, Journ. Quantum Inf. and Comp. **6**(2), 173 (2005).

[13] F. Grasselli, H. Kampermann, D. Bruss, *Conference key agreement with single-photon interference*, New J. Phys **21**, 123002 (2019).

Quantum Blockchains Inc., Lipowa 4a, 20-027 Lublin, Poland
https://quantumblockchains.io/