Quantum Money Scheme: Simulation Results

Jerry Horgan
Walton Institute, Waterford Institute of Technology
jerry.horgan@waltoninstitute.ie

Hazel Murray
Munster Technological University
hazel.murray@mtu.ie

David Malone
Hamilton Institute, Maynooth University
david.malone@mu.ie

Deirdre Kilbane
Walton Institute, Waterford Institute of Technology
deirdre.kilbane@waltoninstitute.ie

ABSTRACT

Quantum computing has the power to break current cryptographic systems, disrupting online banking, shopping, data storage and communications. However, quantum mechanics can also be used to make these systems stronger and more resilient. In this paper we describe the transmissibility of a quantum money scheme, which was proposed by Dmitry Gavinsky and implemented by the authors, and discuss some of its benefits and limitations.

KEYWORDS

Quantum information theory, Quantum money, Digital cash, Quantum simulation, Information-theoretic techniques

ACM Reference Format:
Jerry Horgan, Hazel Murray, David Malone, and Deirdre Kilbane. 2021. Quantum Money Scheme: Simulation Results. In *The Eight Annual ACM International Conference on Nanoscale Computing and Communication (NANOCOM '21), September 7–9, 2021, Virtual Event, Italy*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3477206.3477475

1 INTRODUCTION

Quantum computing has the theoretical power to break certain modern cryptography [6]. In 1994, Peter Shor developed a quantum algorithm that can jeopardise public key cryptographic systems [7], such as RSA. In 1996, Grover's algorithm was developed, which reduced the effectiveness of symmetric key cryptographic systems [4]. Without cryptography, much of our online banking, shopping and data storage technology would no longer be usable.

Though quantum computing has the power to break some of our current systems, it also holds the key to unlocking solutions that exceed the bounds of our current computational capabilities. Quantum technology has particularly useful qualities for applications to communication systems, privacy and security. In particular, the 'no-cloning' theorem, which states that no quantum bit can be duplicated, has been shown to have very useful properties for quantum money [8]. Quantum money was one of the first suggested applications of quantum mechanics in the realm of cryptography. It was first proposed in 1970 by Wiesner but the idea was not accepted for publication until 1983 [8]. This first protocol, which suggests using the basis of the quantum no-cloning theorem as a method of creating unforgeable coins, laid the ground work for the development of the quantum cryptography field.

In this paper, we discuss the transmissiblity of a quantum money scheme proposed by Gavinsky [3]. This scheme allows the issuing of quantum coins, which cannot be cloned and whose validity can be verified by using local quantum operations and a classical channel. This offers efficient coin validation while providing provable security for the coin. We implemented the scheme using the SimulaQron simulator [2]. Source code is available [5].

NANOCOM '21, September 7–9, 2021, Virtual Event, Italy

ACM ISBN 978-1-4503-8710-1/21/09…$15.00
https://doi.org/10.1145/3477206.3477475

2 GAVINSKY'S QUANTUM MONEY

We follow much of Gavinsky's notation. The size of the quantum coin is k, where each coin requires k quantum registers (each consisting of two qubits), a k bit classical register and a unique ID.

To validate one of these coins a coin holder, say Alice, initiates the $\mathcal{V}$er process, see Figure 1. The bank then issues a challenge that begins by choosing a random subset of size t of the k registers and the coin holder must make a measurement on $2t/3$ of these, the local subset.

The details of the measurements and validation involve the use of a quantum *Hidden Matching Problem* called HMP_4 [1].

Gavinsky considers the trade-off between the size of t and k. The larger t is, the harder it is for an attacker to respond to the validation challenge. However, larger t values result in quantum registers being used more quickly, increasing the chance that a legitimate coin holder will be unable to respond to the challenge, and need to have the coin re-issued. A design assumption is that once a quarter of the quantum registers have been used, the coin will be renewed.

Gavinsky shows that if t is chosen to be $\Theta(k^{3/4})$ then $\Omega(k^{1/4})$ validity tests will be possible. Roughly speaking, this means that if we take t proportional to $k^{3/4}$ then the number of validations possible will at least be proportional to $k^{1/4}$.

2.1 Hidden Matching Problem

Verification is based on the Hidden Matching Problem (*HMP*) introduced by Bar-Yossef et al. [1] and defined as follows:

Definition 2.1 (HMP_4 condition). For $x \in \{0,1\}^4$ and $m, a, b \in \{0,1\}$, we say that $(x, m, a, b) \in HMP_4$ if

$$b = \begin{cases} x_1 \otimes x_{2+m} & \text{if } a = 0 \\ x_{3-m} \otimes x_4 & \text{if } a = 1 \end{cases}$$

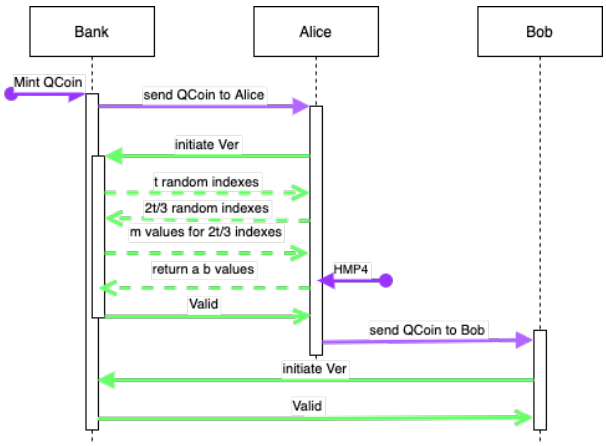

Figure 1: Quantum Coin State Diagram

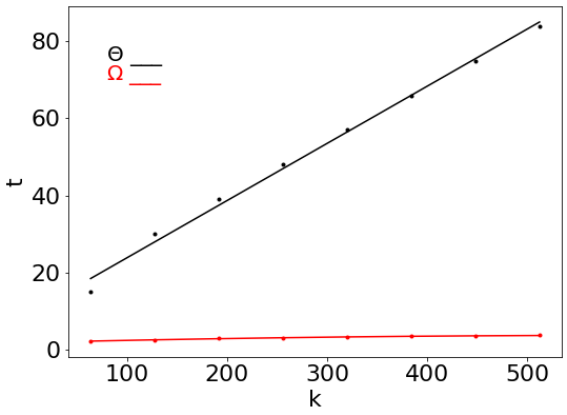

Figure 2: Comparative growth of Ω and Θ

Alice provides classical bit string values (a_i, b_i) to the bank which holds the values m_i. The bank verifies that Alice holds the Q-coin corresponding to the classical values x_i, by verifying $(x_i, m_i, a_i, b_i) \in HMP_4$ for each i in the local subset.

3 DISCUSSION

Gavinsky shows that by choosing a high value of t, such as $t \in \Theta(k^{3/4})$, $\mathcal{V}$er can run $\Omega(k^{1/4})$ times, where it will take $e^{k^{\Omega(1)}}$ time to counterfeit a Q-coin with a probability greater than $e^{-k^{\Omega(1)}}$. In our tests, we initially picked t close to $0.85k^{3/4}$ and found that the constant for the Ω lower bound on completed validations was 0.79.

Figure 2 shows how quickly our t grows in relation to k. Therefore, as the coin size increases so does the number of measurements, t, that are shared with the bank when challenged to $\mathcal{V}$er. However, the number of possible validations does not grow nearly as quickly. Even very large Q-coins, with k = 40,960 the number of possible validations will be proportional to $k^{1/4} = 8$. Though, this will lead to a very small counterfeit probability.

While it is relatively easy to achieve a strong level of security, the Θ bound on the number of validations limits how often the coin can be passed on and validated, which limits the *transmissibility*. In fact, if we follow Gavinsky's recommendation to re-issue the Q-coin after $3k/8t$ successful runs of $\mathcal{V}$er then only 1 or 2 validations can be run. Therefore it is an option for the bank to select the level of security that it desires. The selection of t has an important impact on the re-usability (or transmissibility) of the coin while considering the effort it expends minting (issuing) and transferring the Q-coin. If a transmissibility level of 1 is desired, i.e. to simply prove that you are the holder of a token, then this is easy to achieve. The bank will then need to decide an appropriate counterfeit difficulty level, which would naturally then determine the value of k.

Alternatively, by selecting a Q-coin that takes a smaller proportion of $k^{3/4}$, we would get a coin that could be validated more times and produce a Q-coin with higher transmissibility. Suppose we take $t \approx \alpha k^{3/4}$, where $0 < \alpha < 1$. We get approximately $3k^{1/4}/8\alpha$ validations before Gavinsky recommends re-issuing, which is a slightly conservative lower bound. Or at most we get $3k^{1/4}/2\alpha$ validations before register exhaustion becomes a certainty. For example, using the maximum size we considered, k = 512, and taking $\alpha = 0.527$ we get t = 54, with a maximum transmissibility level of approximately 14, or 3 before Gavinsky recommends re-issuing the Q-coin.

One of the attractive features of Gavinsky's scheme is that the coin does not need to be repeatedly returned to the bank, and the coin holders do not need to have a quantum channel to the bank. Instead they can use untrusted peers such as Bob does with Alice in Figure 1. However, it appears that choosing parameters that allow many validations may be challenging without storing many qubits, making highly transmissible Q-coins a potential challenge.

ACKNOWLEDGEMENT

This publication has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant 13/RC/2077. J. Horgan, H. Murray, D. Malone and D. Kilbane are members of the SFI Research Centre CONNECT. D. Kilbane is funded by SFI (grant no. 18/IF/6357) and is a member of the SFI Research Centre VistaMilk (grant no. 16/RC/3835) and LERO — the Irish Software Research Centre supported, in part, by SFI (grant no. 13/RC/2094).

REFERENCES

[1] Bar-Yossef, Z., Jayram, T. S., and Kerenidis, I. Exponential separation of quantum and classical one-way communication complexity. In *Proc. 36th ACM symposium on Theory of computing* (2004), pp. 128–137.
[2] Dahlberg, A., and Wehner, S. Simulaqron — a simulator for developing quantum internet software. *Quantum Science and Technology 4*, 1 (2018), 015001.
[3] Gavinsky, D. Quantum money with classical verification. In *Proc. 27th Conference on Computational Complexity* (2012), IEEE, pp. 42–52.
[4] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proc. 28th ACM Symposium on Theory of Computing* (New York, NY, USA, 1996), STOC '96, Association for Computing Machinery, p. 212–219.
[5] Horgan, J. Quantum Coin GitHub Repository. https://gitlab-ee.tssg.org/jhorgan/quantum_coin, Nov. 2019.
[6] Mavroeidis, V., Vishi, K., Zych, M. D., and Jøsang, A. The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200* (2018).
[7] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Symposium on Foundations of Computer Science* (1994), IEEE, pp. 124–134.
[8] Wiesner, S. Conjugate coding. *ACM Sigact News 15*, 1 (1983), 78–88.