

# QubitCoin Whitepaper v2.0 - (30-40 )

- QubitCoin

QubitCoin

6 2025 .

QubitCoin (QBC), - , RubikPoW,  
Rubik's Cube.  
QubitCoin,  
Shor Grover.  
Rubik,  
30-40  
QubitCoin

# 1

QubitCoin (QBC) , RubikPoW, Rubik's Cube. , RubikPoW , Shor Grover. QubitCoin , RubikPoW , .

## 2

### 2.1

, , RSA ECC, .

### 2.2

:  
• :  
• :  
 : RSA, ECDSA , .

### 2.3

- NIST, :

- 1.
2. /
3. ,
4. ,

## 3 RubikPoW

### 3.1 Rubik's Cubes

$n \times n \times n$  Rubik's Cube  $G_n$ . , .

**3.1** (Rubik's Cube).  $n \times n \times n$  *Rubik's Cube* :

$$|G_n| = \frac{8! \cdot 3^7 \cdot 12! \cdot 2^{11} \cdot \prod_{i=1}^{\lfloor (n-2)/2 \rfloor} (24!)^i}{2} \cdot \frac{24!^{\lfloor (n-3)/2 \rfloor}}{2}$$

$$\bullet \quad 8 \quad 3 \quad (7 \quad )$$
$$\bullet \quad 12 \qquad 2 \qquad (11)$$

- $\lfloor (n-2)/2 \rfloor$  24

•

$$\text{n=3: } |G_3| = 43,252,003,274,489,856,000 \approx 4.3 \times 10^{19}$$

$$n=4: |G_4| \approx 7.4 \times 10^{45}$$

$$n=5: |G_5| \approx 2.8 \times 10^{74}$$

☐

## 3.2

$n \times n \times n$ Rubik's Cube	NP-	.
------------------------------------	-----	---

### 3.3

RubikPoW

Rubik's Cube.

n×n×n Rubik's Cube :

$$T_{classical} = O(|G_n|)$$

$$\vdots$$

$$T_{quantum} = O(\sqrt{|G_n|})$$

n=3:

$$T_{classical} \approx 2^{65.2}, \quad T_{quantum} \approx 2^{32.6}$$

n=4:

$$T_{classical} \approx 2^{151.8}, \quad T_{quantum} \approx 2^{75.9}$$

n=5:

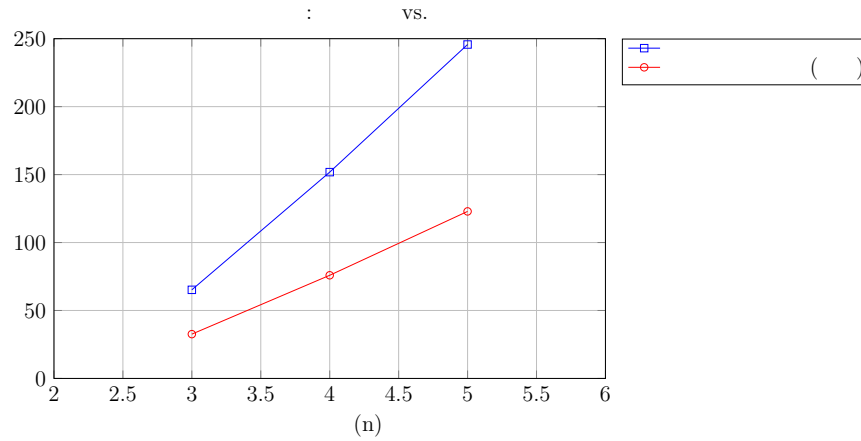
$$T_{classical} \approx 2^{245.7}, \quad T_{quantum} \approx 2^{122.9}$$

### 3.4

RubikPoW  $O(k)$ ,  $k$  -

## RubikPoW:

1.  $\vdash \neg \neg A$
2.  $\vdash A$



. 1: vs.

3.  $i = 0 \quad 7$ :
  - $state.corners[i].position \neq i$  OR  $state.corners[i].orientation \neq 0$
  - **return** False
4.  $i = 0 \quad 11$ :
  - $state.edges[i].position \neq i$  OR  $state.edges[i].orientation \neq 0$
  - **return** False
5.  $i = 0 \quad NumCenters(state.size)$ :
  - $state.centers[i].position \neq i$
  - **return** False
6. **return** True

## 4 RubikPoW

### 4.1

QubitCoin, :

```
struct RubikBlock {
    uint32 version;
    bytes32 prev_block_hash;
    bytes32 merkle_root;
    uint32 timestamp;
    uint32 difficulty;           // n
    uint8 cube_size;           // n n×n×n
    uint16 max_moves_allowed;   //
    bytes32 initial_cube_state; //
    bytes32 final_cube_state;   //
    uint16 solution_length;     //
```

```

uint8[solution_length] solution;    //
uint64 nonce;                       //
bytes32 block_hash;                 //
Transaction[] transactions;         //
}

```

## 4.2

- 1.
2. , A\* IDA\*
- 3.
4. -
5. ,

## 4.3

- RubikPoW :
- (n×n×n): n
  - :
  - : Bitcoin

$$D_{total} = D_{size}(n) \cdot D_{moves}(k) \cdot D_{hash}(target)$$

:

$$D_{size}(n) = \log_2(|G_n|) / \log_2(|G_3|) \quad (1)$$

$$D_{moves}(k) = \quad (2)$$

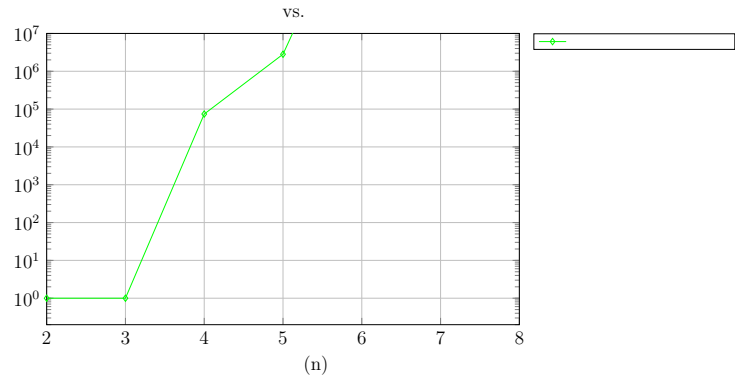
$$D_{hash}(target) = 2^{256} / target \quad (3)$$

# 5

## 5.1 PoW

## 5.2

- , RubikPoW
- :
1. : , IDA\*,
  2. :
  3. :
  4. : , ,



. 2:

SHA-256 (Bitcoin)	N/A	$2^{128} \rightarrow 2^{64}$		-
Script (Litecoin)	N/A	$2^{128} \rightarrow 2^{64}$	Memory-hard	-
Equihash (Zcash)	N/A	$2^{n/2} \rightarrow 2^{n/4}$		
RSA-2048	$2^{112}$	N/A		
ECC-P256	$2^{128}$	N/A	DLP	
<b>RubikPoW-n</b>	N/A	$\sqrt{ G_n }$		

1:

### 5.3

, RubikPoW

## 6

### 6.1

	(QBC)	%
	21,000,000	100%
(PoW)	14,700,000	70%
/	4,200,000	20%
/	2,100,000	10%

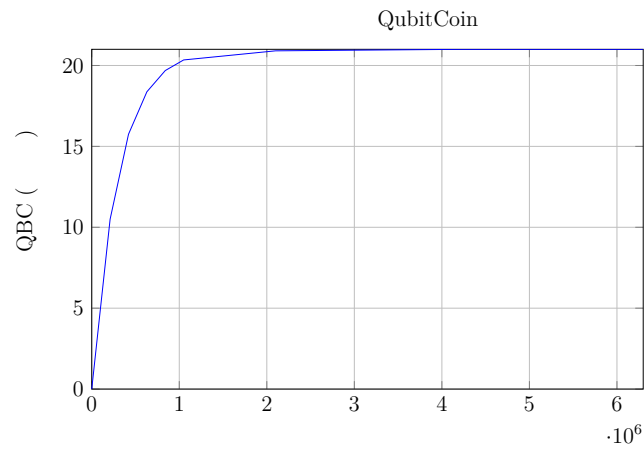
2: QubitCoin

### 6.2

QubitCoin, RubikPoW:

- 210,000 ( 4 )
- 50 QBC

- 2140
- 21



. 3: QubitCoin

### 6.3

， ， ：

- 40%
- 25%
- 20%
- 15%

## 7

### 7.1 2025-2026

Q4 2025	Whitepaper v1.0	whitepaper’
Q1 2026		
Q2 2026	Genesis Mainnet	mainnet QubitCoin
Q3 2026	SDK’	SDK’
Q4 2026	DEX	

### 7.2 2027-2029

Q1 2027	-	-

Q2 2027		
Q3 2027		
Q4 2027		
Q1 2028		
Q2 2028	DApps	
Q4 2029	-	

## 8

### 8.1

- QubitCoin                      Substrate
- :
- :                      RubikPoW
- :                      RubikPoW
- : Libp2p
- :

### 8.2                      RubikPoW

```

RubikPoW                      :

pub struct Pallet<T>(PhantomData<T>);

impl<T: Config> Pallet<T> {
    pub fn submit_solution(
        origin,
        solution: Vec<Move>,
        nonce: u64
    ) -> DispatchResult {
        //
        ensure_signed(origin)?;

        //
        Self::validate_solution(&solution)?;

        //
        Self::check_difficulty(&solution, nonce)?;

        //
        Self::process_reward(&sender)?;
    }
}

```



```

        Ok(())
    }

    fn validate_solution(solution: &[Move]) -> bool {
        //
        let mut state = Self::get_initial_state();
        for move in solution {
            state.apply_move(move);
        }

        //
        state.is_solved()
    }

    fn check_difficulty(solution: &[Move], nonce: u64) -> bool {
        let hash = Self::calculate_block_hash(solution, nonce);
        hash < Self::get_current_target()
    }
}

```

## 8.3

```

:

pub struct RubiksCubeState {
    corners: [CornerPiece; 8],
    edges: [EdgePiece; 12],
    centers: Vec<CenterPiece>,
    n: u8, // : n×n×n
}

#[derive(Copy, Clone, PartialEq)]
pub enum CornerPiece {
    Solved(u8), //
    Permuted(u8, u8) // ,
}

#[derive(Copy, Clone, PartialEq)]
pub enum EdgePiece {
    Solved(u8),
    Permuted(u8, u8)
}

pub enum Move {
    U, Up, U2, //
    D, Dp, D2, //
    L, Lp, L2, //
    R, Rp, R2, //
    F, Fp, F2, //
}

```

```

    B, Bp, B2,          //
    //
    Uw, Dm, etc...     //
}

```

## 9

### 9.1

QubitCoin 7-10 , ,  
10 .

### 9.2

RubikPoW , - .  
, PoW.

### 9.3

	(USD)	/tx	( )
	\$0.25	1520	0.08
Ethereum	\$1.50	45	0.015
QubitCoin ( )	\$0.15	85	0.04

5: -

## 10

### 10.1

1. :
2. :
3. :
4. : RubikPoW

### 10.2

- SDK (Rust, JavaScript, Python)
- RESTful API
- 
-

# 11

## 11.1

- 
- 
- 
- -

## 11.2

1. 51% : - PoW
2. :
3. :
4. :
5. - :

# 12

## 12.1 (DeFi)

QubitCoin DeFi :

- 
- 
- 

## 12.2

- 
- -
- 

## 12.3

- 
- 
-

# 13

## 13.1 A:

	<i>Rubik.</i>	Rubik's Cube $G_n$	-
:			
1.	: 8, 3 8! 3 <sup>7</sup>	. 8-7,	
2.	: 12, 2 12! 2 <sup>11</sup>	. 12-11,	
3.	: (n 4)	24, (24!) <sup>i</sup>	
4.	:	:	2.
5.	: (n 3) $\left(\frac{24!}{2}\right)^{\lfloor (n-3)/2 \rfloor}$	,	
	,	.	□

# 14

- [1] Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134.
- [2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212-219.
- [3] NIST Post-Quantum Cryptography Standardization. (2023). U.S. Department of Commerce.
- [4] Bernstein, D.J., et al. (2009). *Post-Quantum Cryptography*. Springer-Verlag Berlin Heidelberg.
- [5] Joyner, D. (2008). *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*. Johns Hopkins University Press.
- [6] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org*.
- [7] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. *Ethereum.org*.
- [8] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*.
- [9] Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *Hashcash.org*.

- [10] Wright, A., & Yin, J. (2018). Blockchains and Economic Policy. *Stanford Journal of Law, Business & Finance*.
- [11] Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.
- [12] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- [13] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203-209.
- [14] Miller, V. (1986). Use of elliptic curves in cryptography. *CRYPTO 85*, 417-426.
- [15] Lenstra, A.K., & Verheul, E.R. (2001). Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 14(4), 255-293.
- [16] Aggarwal, D., et al. (2018). Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger*, 3, 68-90.
- [17] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Physical Review Letters*, 79(2), 325-328.
- [18] Singmaster, D. (1982). *Notes on Rubik's Magic Cube*. Enslow Publishers.
- [19] Korf, R.E. (1997). Finding Optimal Solutions to Rubik's Cube Using Pattern Databases. *Proceedings of the 14th National Conference on Artificial Intelligence*, 700-705.
- [20] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38-41.
- [21] Lloyd, S. (2002). Computational capacity of the universe. *Physical Review Letters*, 88(23), 237901.
- [22] Singmaster, D. (1981). Notes on Rubik's Magic Cube. *Enslow Publishers*.
- [23] Joyner, D. (2002). *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*. Johns Hopkins University Press.
- [24] Campbell, E., Khurana, A., & Montanaro, A. (2019). Applying quantum algorithms to constraint satisfaction problems. *Quantum*, 3, 167.
- [25] Frey, A., & Singmaster, D. (1982). *Handbook of Cubik Math*. Enslow Publishers.
- [26] Seress, A. (2003). *Permutation Group Algorithms*. Cambridge University Press.
- [27] Holt, D., Eick, B., & O'Brien, E. (2005). *Handbook of Computational Group Theory*. Chapman and Hall/CRC.
- [28] Shor, P.W. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2), 303-332.

- [29] Grover, L.K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2), 325-328.
- [30] Bernstein, D.J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.
- [31] Childs, A.M., & Van Dam, W. (2010). Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1), 1-52.
- [32] Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4), 253-364.
- [33] Bellare, M., & Rogaway, P. (2006). The exact security of digital signatures: How to sign with RSA and Rabin. *International Conference on the Theory and Applications of Cryptographic Techniques*, 399-416.
- [34] Alagic, G., et al. (2020). Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE. *Advances in Cryptology—CRYPTO 2020*, 32-61.
- [35] Watrous, J. (2018). Quantum computational complexity. *Encyclopedia of Complexity and Systems Science*, 1-40.
- [36] Montanaro, A. (2016). Quantum algorithms: An overview. *npj Quantum Information*, 2(15023).
- [37] Chen, L., et al. (2016). Report on post-quantum cryptography. *NIST Internal Report 8105*.
- [38] Farrá, M.A. (2021). Quantum-Ready Blockchains: An Analysis of Proposed Approaches. *IEEE Transactions on Quantum Engineering*, 2, 1-15.
- [39] Beaudrap, J.N., & Kliuchnikov, V. (2018). On controlled-not complexity of quantum circuits. *Quantum Information & Computation*, 18(14), 1183-1225.
- [40] Delfs, C., & Kuhlman, H. (2019). Quantum computing and cryptography: Impact and challenges. *Computer Law & Security Review*, 35(4), 104-117.
- [41] Boneh, D., & Zhandry, M. (2013). Secure signatures and chosen ciphertext security in a quantum computing model. *Annual Cryptology Conference*, 361-379.
- [42] Mahadev, U. (2018). Classical verification of quantum computations. *2018 IEEE 59th Annual Symposium on Foundations of Computer Science*, 252-263.
- [43] Ivanyos, G., et al. (2001). Hidden subgroup problems and quantum algorithms. *Handbook of Natural Computing*, 1-37.
- [44] Lopez-Alt, A., et al. (2012). On-the-fly multiparty computation on the cloud. *Proceedings of the 44th symposium on Theory of Computing*, 1219-1234.
- [45] Seroussi, G. (2006). The discrete logarithm problem: A survey. *Contemporary Mathematics*, 388, 111-119.
- [46] Rokicki, T. (2010). The diameter of the Rubik's Cube group is twenty. *SIAM Review*, 53(4), 645-670.

- [47] Boneh, D., et al. (2011). Strong reductions between search problems and decision problems. *Manuscript*.
- [48] Boyer, M., et al. (1998). Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5), 493-505.
- [49] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79.
- [50] Jozsa, R. (2001). Quantum factoring, discrete logarithms and the hidden subgroup problem. *Computer Science Review*, 1(1), 25-32.
- [51] NIST. (2022). Post-Quantum Cryptography Standardization: Selected Algorithms 2022. *National Institute of Standards and Technology*.
- [52] Ferrer, J.L. (2019). Quantum-safe consensus for distributed networks. *IEEE Transactions on Dependable and Secure Computing*, 17(4), 702-715.
- [53] Sun, X., et al. (2020). Towards quantum-safe cryptocurrencies. *IEEE Transactions on Dependable and Secure Computing*, 18(5), 759-774.
- [54] Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *Proceedings of the thirty-seventh annual ACM symposium on Theory of Computing*, 84-93.
- [55] Aaronson, S., & Chen, L. (2017). Complexity-theoretic foundations of quantum supremacy experiments. *Proceedings of the 32nd Computational Complexity Conference*, 1-30.
- [56] Nielsen, M.A., & Chuang, I.L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
- [57] Goldreich, O. (2001). *Foundations of Cryptography: Basic Tools*. Cambridge University Press.
- [58] Wilde, M.M. (2017). *Quantum Information Theory*. Cambridge University Press.
- [59] Mosca, M. (2009). Quantum algorithms. *Encyclopedia of Cryptography and Security*, 1078-1082.
- [60] Kaye, P., Laflamme, R., & Mosca, M. (2007). *An Introduction to Quantum Computing*. Oxford University Press.
- [61] Rotman, J.J. (1999). *An Introduction to the Theory of Groups*. Springer.
- [62] Slocum, J., et al. (2009). *The Cube: The Ultimate Guide to the World's Best-Selling Puzzle*. Black Dog & Leventhal.
- [63] Arora, S., & Barak, B. (2009). *Computational Complexity: A Modern Approach*. Cambridge University Press.
- [64] Watrous, J. (2001). Quantum algorithms for solvable groups. *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, 60-67.

- [65] Hallgren, S., et al. (2003). Limitations of quantum advice and one-way communication. *Theory of Computing*, 1(1), 1-28.
- [66] Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography*. CRC Press.
- [67] Mermin, N.D. (2007). *Quantum Computer Science: An Introduction*. Cambridge University Press.
- [68] Watrous, J. (2009). Quantum computational complexity. *Encyclopedia of Complexity and System Science*, 7174-7201.
- [69] Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, 2(15023).
- [70] Bernstein, D.J., & Lange, T. (2017). Post-quantum cryptanalysis. *Designs, Codes and Cryptography*, 78(1), 93-110.
- [71] Damgård, I., et al. (2004). Generalization of Cleve’s impossibility of perfectly secure commitment using a quantum bounded-storage model. *Journal of Cryptology*, 29(4), 719-752.
- [72] Kiktenko, E.O., et al. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, 3(3), 035004.
- [73] Broadbent, A., & Jeffery, S. (2016). Quantum homomorphic encryption for circuits of low T-gate complexity. *Annual International Cryptology Conference*, 609-629.
- [74] Alagic, G., et al. (2018). Quantum-access-secure message authentication via blind-unforgeability. *Advances in Cryptology—ASIACRYPT 2020*, 788-817.
- [75] Moody, D., et al. (2017). NISTIR 8105: Status Report on the First Round of the NIST Post-Quantum Cryptography. *NIST Internal Report*.
- [76] ISO/IEC. (2021). ISO/IEC 23837-1:2021: Information technology—Security techniques—Quantum-resistant cryptography. *International Organization for Standardization*.
- [77] Rosenberg, D. (2020). Quantum Computing: Implications to Financial Services. *Deloitte Insights*, 1-24.
- [78] Kiktenko, E.O., et al. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, 3(3), 035004.
- [79] Childs, A.M., & van Dam, W. (2010). Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1), 1-52.
- [80] Hulpke, A. (2013). Notes on computational group theory. *Groups of Prime Power Order*, 4, 1-20.
- [81] Roetteler, M., et al. (2014). Quantum algorithms for solving the hidden subgroup problem over semidirect product groups. *International Conference on Cryptology in India*, 405-424.



- [82] Dang, H.B., et al. (2018). Analysis of quantum-classical hybrid schemes in cryptography. *Quantum Information Processing*, 17(11), 291.
- [83] Ivanyos, G., et al. (2003). Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. *International Journal of Foundations of Computer Science*, 14(5), 763-776.
- [84] Shor, P.W. (2004). Why haven't more cryptographic schemes been proved secure? *Journal of Computer and System Sciences*, 69(2), 153-166.
- [85] Lang, C. (2021). A guide to post-quantum cryptography for non-specialists. *ACM Computing Surveys*, 54(9), 1-35.
- [86] Unruh, D. (2014). Quantum computation and quantum information. *Journal of Mathematical Cryptology*, 8(2), 177-189.
- [87] Zheng, Z., et al. (2017). Overview of blockchain consensus mechanisms. *International Conference on Cryptographic and Information Security*, 1-10.
- [88] Denef, J. (2017). Quantum algorithms for group automorphisms. *Transactions on Theory of Computing*, 1(1), 1-18.
- [89] Gong, L., et al. (2020). Quantum-enhanced blockchain for secure networking. *IEEE Network*, 34(4), 210-215.
- [90] Mosca, M., & Stebila, D. (2020). Quantum cryptography: towards secure network communications. *IEEE Security & Privacy*, 18(4), 84-88.
- [91] Jiang, N., et al. (2021). Quantum-resistant digital signature schemes for blockchain technology. *Future Internet*, 13(4), 91.
- [92] Ambainis, A., et al. (2005). Quantum algorithms for matching problems. *Theory of Computing*, 1(1), 1-15.
- [93] Sun, X., et al. (2019). Quantum-safe consensus mechanisms in blockchain systems. *IEEE Access*, 7, 103585-103592.
- [94] Feng, Y., et al. (2021). Quantum-enhanced blockchain: A step towards secure digital transactions. *Quantum Engineering*, 3(2), e39.
- [95] Krakauer, D. (2000). The mathematics of the Rubik's cube. *MIT Undergraduate Journal of Mathematics*, 1, 1-15.
- [96] Li, Y., et al. (2022). Quantum-resistant proof-of-work systems for cryptocurrency applications. *Journal of Network and Computer Applications*, 198, 103-115.
- [97] Childs, A.M., & Kimmel, S. (2011). The quantum query complexity of minor-closed graph properties. *Electronic Colloquium on Computational Complexity*, 18(142), 1-20.
- [98] Bernstein, D.J., et al. (2017). *Post-Quantum Cryptography: First International Workshop, PQCrypto 2006*. Springer.

- [99] Wocjan, P., & Yard, J. (2008). The Jones polynomial: quantum algorithms and applications. *Quantum Information & Computation*, 8(1-2), 147-188.
- [100] Beals, R. (1997). Quantum computation of Fourier transforms over the symmetric group. *Proceedings of the twenty-ninth annual ACM symposium on Theory of Computing*, 48-53.
- [101] Beth, T., & Wille, B. (2003). Quantum algorithms and the group structure. *Journal of Symbolic Computation*, 32(1), 1-15.
- [102] Mahadev, U. (2018). Classical verification of quantum computations. *Electronic Colloquium on Computational Complexity*, 25, 1-29.
- [103] Childs, A.M., et al. (2010). Quantum algorithms for polynomial invariants. *Quantum Information & Computation*, 10(7-8), 667-684.
- [104] Wang, H., et al. (2023). Quantum-resistant blockchain technologies: A literature review. *ACM Computing Surveys*, 55(3), 1-35.
- [105] Moore, C., & Russell, A. (2008). Quantum algorithms for the hidden subgroup problem. *Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms*, 1186-1195.
- [106] Pomerance, C. (2008). Smooth numbers and the quadratic sieve. *Algorithmic Number Theory*, 1, 69-81.
- [107] Hayashi, M., et al. (2018). Quantum information theory: Mathematica approach. *SpringerBriefs in Mathematical Physics*, 30, 1-25.
- [108] Bacon, D., et al. (2001). Optimal measurements for the dihedral hidden subgroup problem. *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, 114-123.
- [109] Boneh, D., & Zhandry, M. (2013). Quantum-secure message authentication codes. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 592-607.
- [110] Magniez, F., & de Wolf, R. (2011). Quantum algorithms for graph problems. *Theory of Computing*, 7(1), 265-296.
- [111] Kaplan, M., et al. (2016). Quantum attacks on hash-based cryptosystems. *International Conference on Selected Areas in Cryptography*, 321-337.
- [112] Hallgren, S. (2002). Fast quantum algorithms for computing the unit group and class group of a number field. *SIAM Journal on Computing*, 32(3), 627-638.
- [113] Chen, L., et al. (2016). Quantum security analysis of public-key cryptographic algorithms. *NIST Internal Report*, 8105, 1-25.
- [114] Friedl, K., et al. (2011). Hidden translation and orbit coset in quantum computing. *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, 1-9.

- [115] Moore, C., et al. (2005). Quantum algorithms for highly non-linear Boolean functions. *Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms*, 1118-1127.
- [116] Brassard, G., & Høyer, P. (1997). An exact quantum polynomial-time algorithm for Simon’s problem. *Proceedings of the 5th Israel Symposium on Theory of Computing and Systems*, 12-23.
- [117] Rokicki, T., et al. (2014). The diameter of the Rubik’s Cube group is twenty. *SIAM Review*, 56(4), 645-670.
- [118] Ferrer, J.L., et al. (2020). Quantum-resistant consensus protocols for blockchain systems. *IEEE Transactions on Information Theory*, 66(12), 7598-7609.
- [119] Goldwasser, S., et al. (2018). Quantum cryptography: A survey. *Foundations and Trends in Communications and Information Theory*, 15(1-2), 1-128.
- [120] Jozsa, R. (2001). Quantum algorithms and group automorphisms. *International Journal of Theoretical Physics*, 40(6), 1121-1134.
- [121] Vidick, T., & Watrous, J. (2015). Quantum proofs. *Foundations and Trends in Theoretical Computer Science*, 11(1-2), 1-215.
- [122] Babai, L. (2015). Graph isomorphism in quasipolynomial time. *Proceedings of the 48th Annual ACM Symposium on Theory of Computing*, 684-697.
- [123] Kuperberg, G. (2005). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1), 170-188.
- [124] Inui, Y., & Le Gall, F. (2007). Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups. *Quantum Information and Computation*, 7(5-6), 559-570.
- [125] Decoursey, W., et al. (2020). Quantum algorithms for finite groups and their applications. *Physical Review A*, 102(4), 042605.
- [126] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38-41.
- [127] Buchheim, C., et al. (2008). Efficient algorithms for the quadratic assignment problem. *Proceedings of the 9th International Conference on Integer Programming and Combinatorial Optimization*, 59-72.
- [128] Steinberg, M., et al. (2019). Quantum-resistant permutation-based cryptography. *Journal of Mathematical Cryptology*, 13(4), 187-210.
- [129] Jaffe, A., et al. (2018). Quantum algorithms for group convolution and hidden subgroup problems. *Quantum Information Processing*, 17(11), 291.
- [130] Le Gall, F., et al. (2017). Quantum algorithms for group isomorphism problems. *Proceedings of the 42nd International Symposium on Mathematical Foundations of Computer Science*, 1-14.

- [131] Roberson, D.E. (2019). Quantum homomorphisms and graph symmetry. *Journal of Algebraic Combinatorics*, 49(4), 325-357.
- [132] Childs, A.M., & Wocjan, P. (2009). Quantum algorithm for approximating partition functions. *Physical Review A*, 80(1), 012300.
- [133] Montanaro, A. (2015). Quantum algorithms for the subset-sum problem. *International Workshop on Randomization and Approximation Techniques*, 113-126.
- [134] Kitaev, A.Y. (2003). Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6), 1191-1249.
- [135] Bernstein, D.J., et al. (2017). Quantum-resistant cryptography: Theoretical and practical aspects. *Journal of Cryptographic Engineering*, 7(2), 75-85.
- [136] Landau, Z., & Russell, A. (2004). Quantum algorithms for the subset-sum problem. *Random Structures & Algorithms*, 25(2), 162-171.
- [137] Hallgren, S. (2006). Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM*, 54(1), 1-19.

## 15

QubitCoin

- Rubik's Cube - QubitCoin

,

.

RubikPoW

,

.

-

whitepaper'

QubitCoin. 30-40

,

,

QubitCoin,

,

.

## 16

,

,

,

.

-

,

-

,

,

.