Blockchain-Enabled Distributed Rummy: Proof for the Designers in Online Skill Gaming Industries

Debendranath Das, Subhamoy Maitra

Indian Statistical Institute, Kolkata, India.

25th International Conference on Cryptology in India
INDOCRYPT 2024

Roadmap

- Introduction
- Challenges in Online Rummy Platforms
- Motivation for Blockchain Based Solution
- Blockchain & Smart Contract
- How to play Rummy
- Description of Proposed Protocol
- Security and Fairness Aspects
- Implementation & Experimental Results
- Conclusion & Future Work
- Reference

Introduction

- **Rummy: A Game Loved by Generations**
  - ✓ Originating centuries ago, rummy is believed to have roots in Mexico's Conquian and China's Mahjong.
  - ✓ Today, it's one of the most popular card games worldwide, blending strategy, skill, and a dash of luck.
  - ✓ In India, online rummy is a $335 million industry, growing at 35% annually.
- **The Thrill of Online Rummy**
  - ✓ Convenience: Play anytime, anywhere.
  - ✓ Competition: Real-time matches with players across the globe.
  - ✓ Stakes: Skill meets reward—but fairness is often questioned.
- **The Big Question:**
  - ✓ Can you trust a dealer who controls every aspect of the game?
  - ✓ What if you could play rummy with zero fear of manipulation?

Pure Sequence
Impure Sequence
Set 1
Set 2
3
4
5
6
A
8
3
K
K
K
5
5
JOKER

https://www.rummycircle.com/how-to-play-rummy/rummy-rules.html

Challenges in Online Rummy Platforms

- Lack of transparency in card distribution.
- Use of bots or fake players.
- Manipulation of Random Number Generators (RNGs).
- Monopolistic dealer control.
- Legal and ethical concerns.

https://thumbs.dreamstime.com/b/medicine-healthcare-people-concept-doctor-displeased-male-patient-arguing-clinic-doctor-displeased-male-patient-107385320.jpg

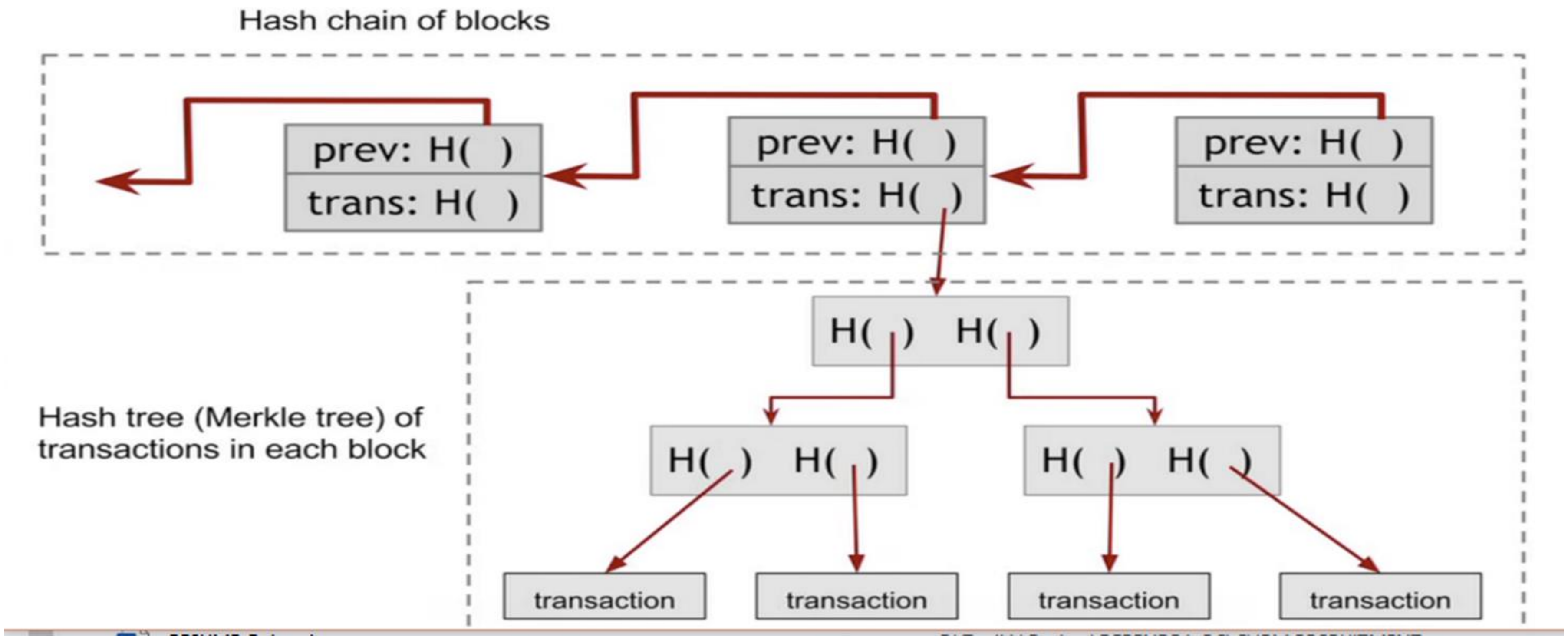
Motivation for Blockchain Based Solution

- Decentralized control eliminates dealer’s monopolization.
- Transparent processes ensure fairness.
- Increases trust among the players.
- Immutable records prevent manipulation.

https://blog.advancedresources.com/hubfs/blog-importanceoftransparency.png

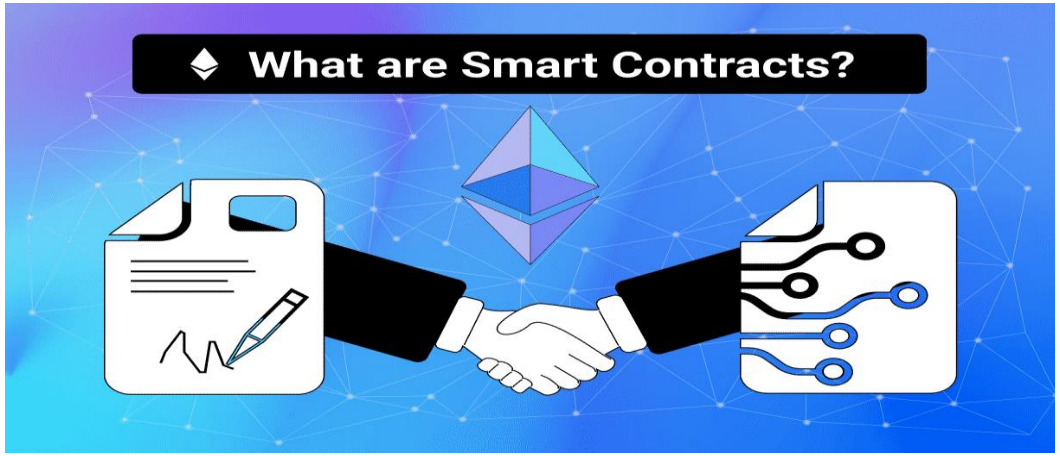
Introdution to Blockchain

- A blockchain is “an **open distributed ledger** that can record transactions between two parties **efficiently** and in a **verifiable** and **permanent** way”- Lsnsiti, Lakhani 2017



Smart Contracts

- “Code is Law” – Unambiguous agreement
- Computer programs - Logical
- Stored on blockchain - immutable
- Can be executed automatically – eliminates TTP
- Trigger transactions in the blockchain network



https://blockgeeks.com/wp-content/uploads/2016/10/What-are-Smart-Contracts_.png

How to Play Rummy?

1. **Dealing Cards:**
   - Each player is dealt 13 cards. The remaining cards form the closed deck, and the top card is placed face-up to start the open deck.
2. **Player's Turn:**
   - Each player, in turn, performs the following:
     - I. **Draw a Card:** Pick one card from either the closed or open deck.
     - II. **Organize Cards:** Arrange cards into valid combinations:
       - a) **Set:** A group of 3 or 4 cards of the same rank but different suits (e.g., 7♥, 7♠, 7♦).
       - b) **Sequence:** A consecutive group of cards from the same suit:
         - ✓ **Pure Sequence:** No joker is used (e.g., 4♠, 5♠, 6♠).
         - ✓ **Impure Sequence:** Includes a joker as a substitute (e.g., 7♥, 8♥, Joker).
3. **Discard a Card:**
   - The player discards one card to the open deck.
4. **Declare:**
   - Once all cards are arranged into valid sets and sequences (with at least one pure sequence), the player declares their hand.
5. **Winning:**
   - If the declaration is valid, the player wins. If not, the game continues until another valid declaration is made.

Proposed Protocol

- **Actors:** Players, Dealer
- **Smart Contracts**: Smart Contract (SC_Rummy)
- **Combines on-chain and off-chain processes.**
- **Key phases:**
  1. Shuffling of Cards.
  2. Distribution of Cards.
  3. Drawing and Discarding Cards.
  4. Endgame Verification.

Phase 1: Shuffling Cards

- **Goal:** Ensure unbiased shuffling, where no single entity controls the shuffle.
- **Process:**
  1. **Seed Generation:**
     I. Players $P1, P2, \ldots, Pn$ generate random seeds $S1, S2, \ldots, Sn$.
     II. Dealer D generates a secret seed Sd.
  2. **Commitment:**
     I. Players and dealer submit hashed commitments $H(Si)$ and $H(Sd)$ to smart contract.
  3. **Initial Hash Calculation:**
     I. A combined hash is generated:
        initial_hash = $H(S1 \,||\, S2 \,||\ldots||\, Sn \,||$ block.timestamp || block.number)
  4. **Final Hash:**
     I. Dealer contributes Sd to calculate the final shuffle hash:
        final_hash=H(initial_hash || Sd)
  5. **Shuffling Algorithm:**
     I. Cards $c1, c2, \ldots, c104$ are permuted using final_hash with a deterministic algorithm.
- **Outcome:** An unpredictable and verifiable shuffle is created.

Phase 2: Distribution of Cards

Phase 3: Drawing & Discarding Cards

- **Goal:** Ensure fairness and transparency in card drawing and discarding.
- **Process:**

  1. **Drawing a Card:**

     I. Player *Pi* requests a card from the closed deck.

     II. Dealer commits the hash of the card (ci) combined with the secret seed *Sd*: $H(ci \,||\, Sd)$

     III. Dealer encrypts the card using *Pi*'s public key $E_{\ddot{i}}\,Z_i(ci)$, and sends it to *Pi*.

  2. **Verification by Player:**

     I. *Pi* decrypts $E_{\ddot{i}}\,Z_i(ci)$, using their private key *SKi* and commits: $H(ci \,||\, Si')$

     II. *Si'* is a fresh seed generated by *Pi*.

  3. **Discarding a Card:**

     I. *Pi* announces the discarded card publicly.

- **Outcome:** Verifiable card draws and discards ensure transparency and fairness.

Phase 4: End Game Verification

- **Goal:** Verify the integrity of the shuffle, distribution, and gameplay.
- **Process:**

  1. **Seed Reveal:**
     - I. Dealer reveals Sd, and players reveal their seeds $S1, S2, \ldots, Sn$ on Smart Contract.
     - II. Smart contract verifies the commitments:

       $H(Sd)$ =? committed $H(Sd)$, $H(Si)$ =? committed $H(Si)$
  2. **Deck Reconstruction:**
     - I. Players reconstruct the final shuffle using:

       final_hash = H(initial_hash || Sd)
  3. **Merkle Tree Validation:**
     - I. Verify the order of the closed deck cards using the Merkle root.
     - II. Each leaf node represents a card hashed with the dealer's secret seed: $H(ci \,||\, Sd)$
  4. **Result Verification:**
     - I. Players validate their hands and drawn cards by comparing committed hashes.

- **Outcome:** Complete transparency and auditability of gameplay.

Security & Fairness Aspects

- **Fairness**
  - ✓ Decentralized shuffling and endgame verification ensure transparency and prevent manipulation.

- **Privacy**
  - ✓ Encrypted card hands protect player information, with hidden dealer seeds ensuring unpredictable shuffles.

- **Data Security**
  - ✓ Immutable blockchain records and commitment schemes safeguard the game's integrity.

Implementation & Experimental Results

Implementation Setup:

- We have implemented the protocol in a system having Intel(R) Core(TM) i5-8250U running Linux Ubuntu 22.04.2, a 64-bit operating system using 8.00GiB of RAM.

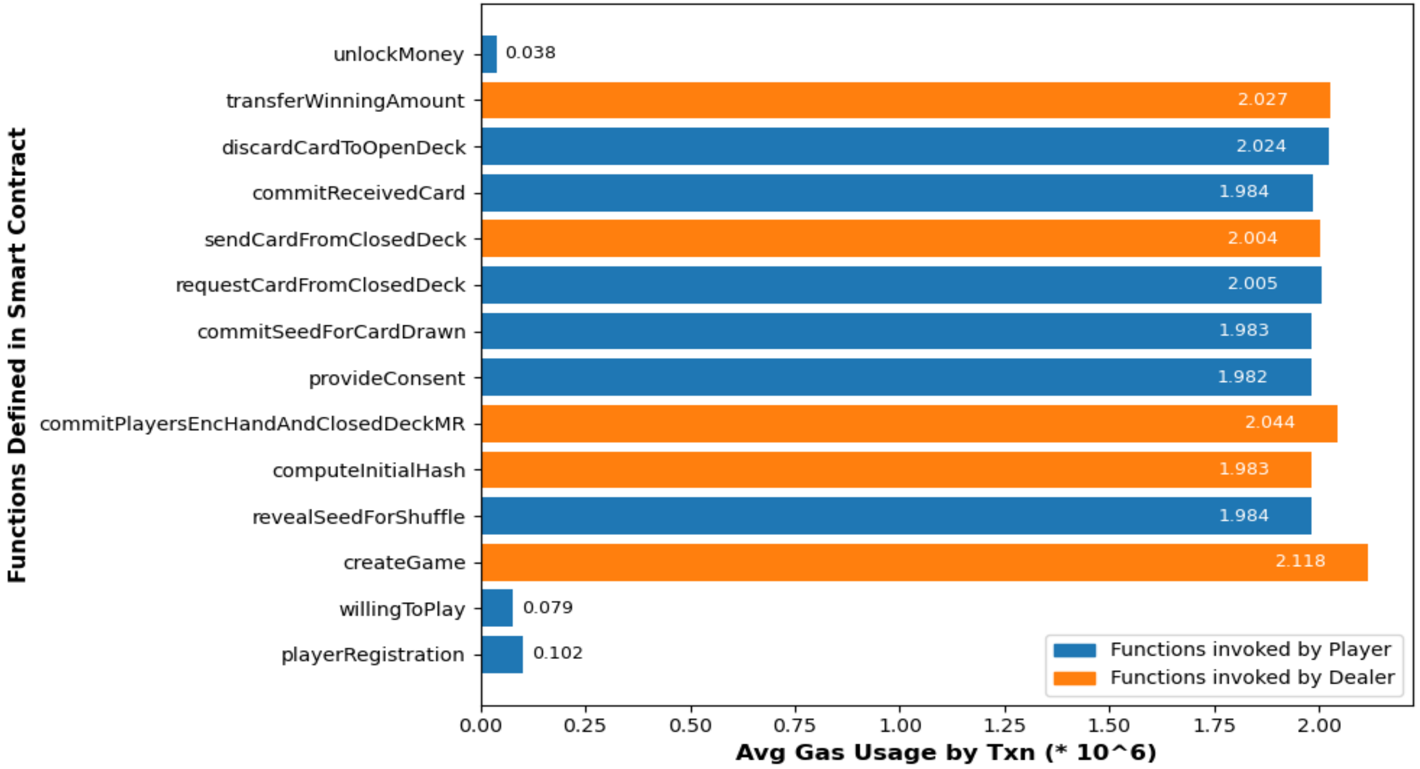
- We have deployed our smart contract on Ethereum Test Network – Sepolia. The Deployment Address of the Smart Contract is given below.

Smart Contract	Address
SC_Rummy	0xff677e8eb96da152f8d880ebe60a5141027bcf82

- The Source code is publicly available on GitHub (https://doi.org/10.5281/zenodo.13985217).

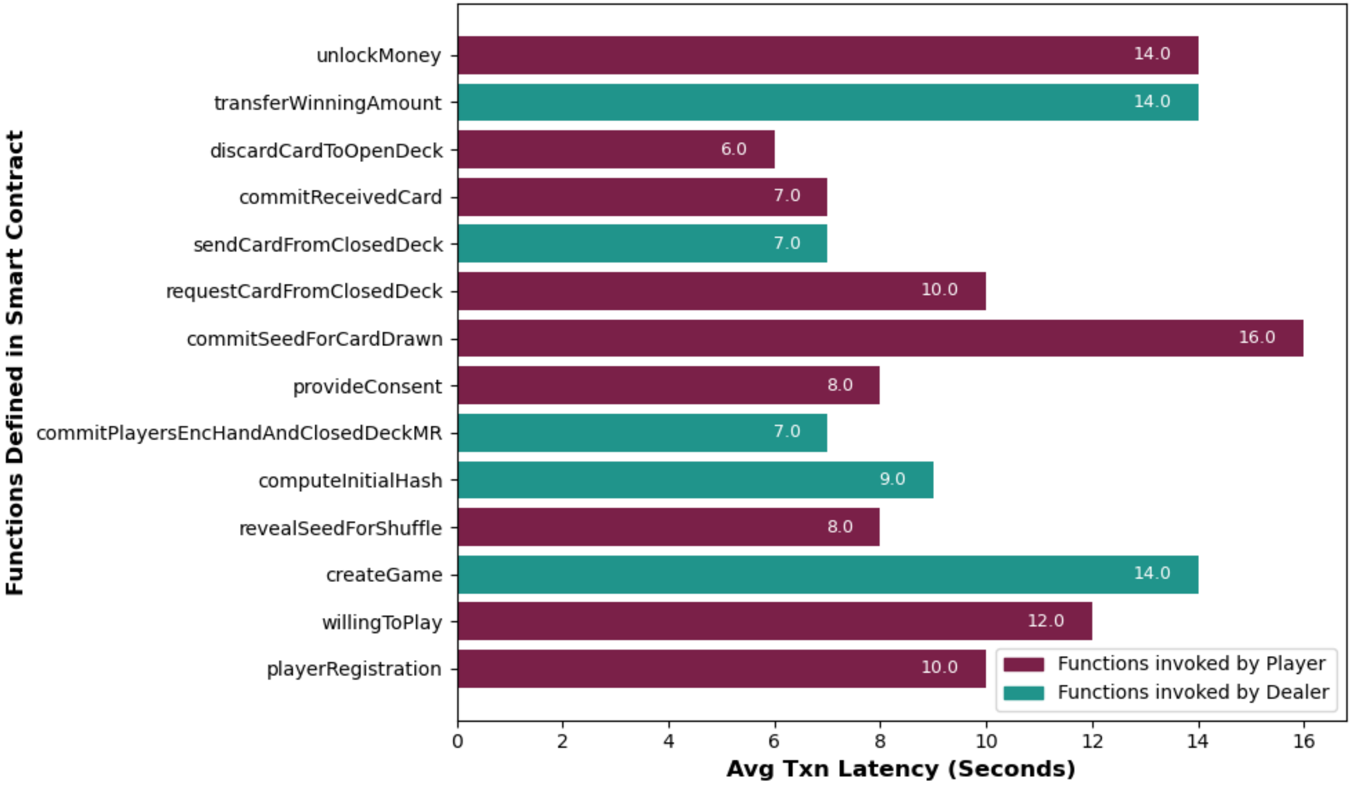
Implementation & Experimental Results Contd.

✓**Transaction Cost:** The execution of a transaction within the Ethereum ecosystem incurs a fee known as gas. Gas refers to the monetary cost associated with completing a transaction or the execution of a contract on the Ethereum platform.



Implementation & Experimental Results Contd.

- ✓**Transaction Latency:** Latency refers to the duration of time that a user must wait after initiating a transaction by broadcasting it to the network before it is processed and then included in a block



Conclusion

- We introduced a blockchain-enabled distributed system for online rummy platforms so that the dealer can efficiently convince the community regarding fairness.
- Our approach ensures that key game actions such as card shuffling, card distribution, and card drawing can be managed transparently and verifiably, enhancing fairness and trust among players.
- Demonstrated feasibility on Ethereum platform.
- Highlights potential for broader gaming applications.

Future Work

- **Challenges & Limitations**
  - Gas fees increase operational costs.
  - Public blockchain latency impacts real-time gameplay.
  - Scalability and usability challenges in adoption.

- **Future Directions:**
  - Explore zero-knowledge proofs for enhanced privacy.
  - Investigate secure multi-party computation (SMPC).
  - Develop consortium blockchains for industry adoption.

References

1. Bach, L.M., Mihaljevic, B., Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1545–1550. IEEE (2018). https://doi.org/10.23919/MIPRO.2018.8400278

2. Boneh, D., Shoup, V.: A Graduate Course in Applied Cryptography, Draft 0.5 (2020).

3. Das, D.: BISECTION: BlockchaIn-enabled SECure healTh Insurance prOcessiNg. International Journal of Ad Hoc and Ubiquitous Computing 46(1), 44–63 (2024). https://doi.org/10.1504/IJAHUC.2024.138744

4. Allende, M., León, D.L., Cerón, S. et al.: Quantum-resistance in blockchain networks. Sci Rep 13, 5664 (2023). https://doi.org/10.1038/s41598-023-32701-6

5. Hewa, T., Ylianttila, M., Liyanage, M.: Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications 177, 102857 (2021). https://doi.org/10.1016/j.jnca.2020.102857

6. Jing, S., Zheng, X., Chen, Z.: Review and investigation of Merkle tree's technical principles and related application fields. In: 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), pp. 86–90. IEEE (2021). https://doi.org/10.1109/CAIBDA53561.2021.00026

7. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. 2nd edn. CRC Press (2020).

8. Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., Bani-Hani, A.: Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications 14(5), 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

9. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton (2016).

10. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Business & Information Systems Engineering 59(3), 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3

11. Preneel, B.: Hash Functions. Springer US, Boston, MA (2011). https://doi.org/10.1007/978-1-4419-5906-5_580, https://doi.org/10.1007/978-1-4419-5906-5_580

12. Stinson, D.R., Paterson, M.: Cryptography: Theory and Practice. 4th edn. CRC Press (2018).

13. Szydlo, M.: Merkle tree traversal in log space and time. In: Advances in Cryptology – EUROCRYPT 2004, vol. 3027, pp. 541–554. Springer (2004).

References

14. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials 22(2), 1432–1465 (2020). https://doi.org/10.48550/arXiv.1904.04098

15. https://www.business-standard.com/industry/news/pm-narendra-modi-calls-for-india-to-lead-the-race-in-gaming-market-124081500753_1.html, August 15, 2024.

16. https://www.rassociates.in/the-legality-of-online-rummy-in-india/, September 7, 2023.

17. https://www.hindustantimes.com/ht-insight/future-tech/objective-metrics-for-regulation-in-the-online-gaming-industry-101714742484953.html, May 3, 2024.

18. https://indianexpress.com/article/cities/ahmedabad/gnlu-gaming-regulations-india-industry-risks-9550388/, September 4, 2024. Full report available at https://gnlu.ac.in//Document/content-docs/1b3b905c-7d50-48c1-b6c0-5dbada252935.pdf

19. E-Gaming Federation. https://www.egf.org.in/

20. All India Gaming Federation. https://aigf.in/

21. https://www.rummycircle.com/how-to-play-rummy/rummy-rules.html

22. https://www.jungleerummy.com/

23. Das, D.: Blockchain-Enabled-Distributed-Rummy-Proof-for-the-Designers-in-Online-Skill-Gaming-Industries: Blockchain-Enabled Distributed Rummy: Proof for the Designers in Online Skill Gaming Industries (v1.0.0)., Zenodo (2024), https://doi.org/10.5281/zenodo.13985217

24. https://www.clarisco.com/case-study/crypto-based-payment-gateway-platform-for-online-rummy-game

25. https://www.alwin.io/rummy-dapp-game-development-company

26. https://rummyverse.com/blogs/blockchain-and-rummy

27. Garg S, Kate A, Mukherjee P, Sinha R, Sridhar S.: Insta-Pok3r: Real-time Poker on Blockchain. Cryptology ePrint Archive (2024)

28. Chan Yip Hon B, Zaghdoudi B, Potop-Butucaru M, Tixeuil S, Fdida S.: Challenger: blockchain-based massively multiplayer online game architecture. In: International Conference on Networked Systems, pp. 50–66. Cham: Springer Nature Switzerland (2024). https://doi.org/10.1007/978-3-031-67321-4_3

Thank You