Police FIR Registration and Tracking Using Consortium Blockchain

Vikas Hassija[1], Aarya Patel[1], and Vinay Chamola[2]

[1]Department of CS and IT, JIIT, Noida, India
[2] Department of Electrical and Electronics Engineering, BITS - Pilani, Pilani campus, India
{vinay.chamola@pilani.bits-pilani.ac.in}

Abstract. India is a developing country, and technology has played a major role in its development. We can see technological advancements in many areas, such as education, business, medical, banking, agriculture, etc. Unfortunately, the Indian Police Department remains devoid of technology in their systems up to certain extents. Also, with the rapid increase in population, the crime rates have increased. Therefore it has become a gruelling task to manage these documents manually. The conventional system of visiting a police station for registering a First Information Report(FIR) or police complaint and getting updates needs to be replaced with a more convenient and transparent system. Hence, we propose a consortium blockchain architecture for the Indian Police Department, where all the police stations will be a part of this network. Consortium blockchain benefits from the privacy of private blockchain while leveraging the decentralized governance of public blockchain. In our proposed system, the client can register their FIR using a decentralized application. Our system ensures its acceptance and timely updates to be delivered to the victims. The scenario of FIR requires a highly secure and trustworthy workflow that has to be fast enough simultaneously.

Keywords: Consortium blockchain, FIR tracking, Smart contracts, Consensus algorithms, Data privacy.

1 Introduction

We have proposed this system keeping in mind the difficulties that people face during the registration of an FIR or a complaint at the police station[1]. In the conventional system, the people have to physically visit the police station multiple times, which is very time-consuming. The same also consumes a whole lot of money and energy. The other disadvantages include the fear of getting abused or harmed by people against whom FIR is lodged. Filing FIR against a highly reputed person is sometimes a hard task. It is a common issue that people are often refused an FIR registration. The possible reasons could be that the police official genuinely does not believe the informant, or it could be that his refusal stems from

the influence upon him of powerful vested personnel, who have managed to approach him before the informant. The Indian Legal System provides some options that one can exercise in such cases, but it is often seen that people don't have the required information, time, energy, and money to exercise the same. By allowing people to file their complaints directly, this system bypasses the police officers who are often reluctant to register the FIRs, mainly in kidnapping and ransom cases. This would also help eliminate corruption.

In recent years, blockchain technology [2], [3] has attracted increased interests worldwide in various domains such as finance, insurance, energy, logistics, and mobility. It has the potential to revolutionize the way applications will be built, operated, consumed, and marketed in the near future. In this context, consortium blockchains [4] emerged as an interesting architecture concept that has some advantages of both the private and the public blockchains. These consortium blockchains can also be described as being semi-decentralized. They possess the security features that are inherent in public blockchains, whilst also allowing for a greater degree of control over the network [5], [6]. Proper maintenance of Police Station records is a prerequisite for the smooth functioning of a police station. However, nowadays, these records are highly vulnerable and are exposed to the risk of being breached or forged. Our proposed system would ensure transparency, security, and privacy of the records stored [7]. The verification of the transaction information would require a consensus mechanism. Current consensus mechanisms designed for blockchains are slow due to the significant amount of time and energy consumed for block production, and safety. Therefore our objective is to design a consensus algorithm with high performance to be used in consortium blockchain [8]. In this paper, we propose a Proof of Vote consensus protocol based on voting mechanism and consortium blockchain.

2 Proposed Solution

We propose to develop a system wherein the victim can lodge their FIR using a mobile application. As shown in Fig1, the victim would fill up the FIR form on his mobile application. He would provide the proofs and details related to the complaint in the application. The user can upload images, audio files, and video files as records. These details would then be converted into a transaction, with the digital signature of the complainant and a smart contract [9] would also be associated with it. The transaction will now float in the network of consortium. The commissioner (the head of a police station) of the respective police station can go through all the FIRs registered at his police station and assign police inspectors (miner candidates) in-charge of the floating FIRs by directly messaging them through the app. All the police inspectors will have a score according to the work they perform. If the inspector in-charge fails to provide updates to the

complainants, then the smart contract, which has a certain time limit by design, would notify the

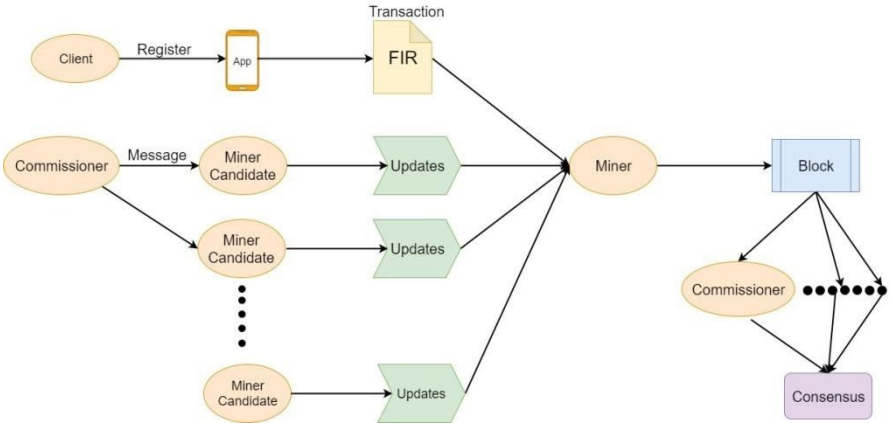

Fig. 1. The flow of the proposed solution.

commissioner about the failure of the inspector in-charge. The commissioner now will decrease the score of that police inspector. Based on this score, the commissioner would select a group of miners whose work would be to collect all the floating transactions and combine them into a block and send it to all the commissioners in the network for verification. The scoring system would ensure honest behaviour on the part of the police officials. The commissioner would now validate the transactions in the block. If any transaction is found invalid, then the police inspector who formed this transaction would be held responsible, and the commissioner would take actions against him accordingly. Fig. 1 shows the flowchart of the process to be followed to FIR registration and tracking in the proposed model.

3 Network Architecture

A consortium blockchain is a specialized blockchain with authorized nodes to maintain distributed shared databases [10], [11]. As our system is a consortium blockchain, it becomes very important to keep it distributed so that a singular entity does not possess all the power. To solve this problem, we have proof of Vote as the consensus mechanism [12]. Consensus participants of a consortium blockchain are likely to be a group of pre-approved nodes on the network. Thus, consortium blockchain possesses the security [13], [14] features that are absent in public blockchain while allowing the required degree of control over the network [15], [16].

3.1 Consortium Blockchain Model

In our blockchain system, we have established different roles for the network participants that have been divided on the basis of their functionality. Fig. 2 shows

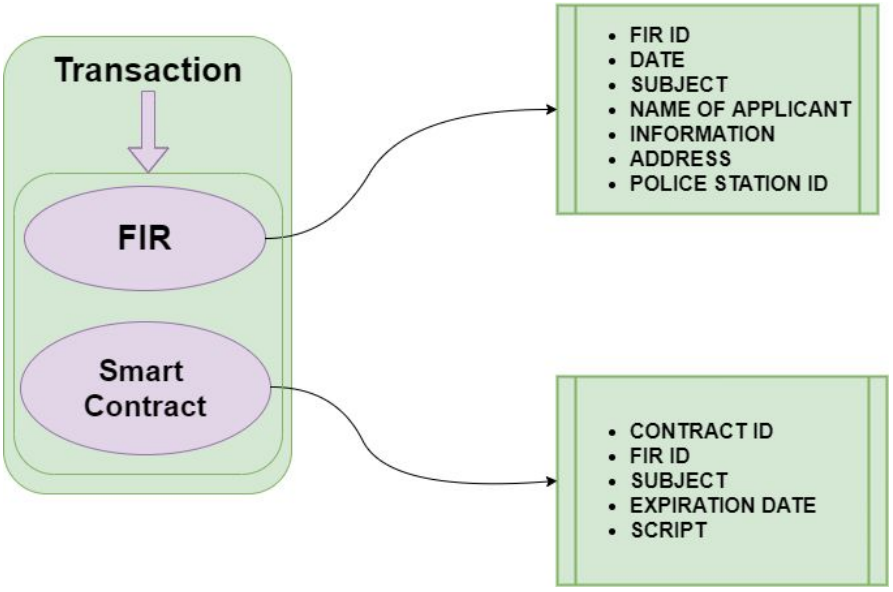

Fig. 2. Format of transactions on the blockchain.

the format of a single transaction added in the blockchain for an FIR. The four roles are:

1. **Commissioner: -** Just like in the real world, the commissioner in our consortium blockchain will have the right to recommend and vote miners to form a blockchain. They will have the power to choose a miner from all the miner nodes to form a block from the floating transactions. With that, they are also given the power to evaluate the transactions (FIR transaction from the client or case update from miner candidate) inside the block made by the miners. The blocks made by the miners will be considered valid and will get added to the longest chain of blockchain only when it will receive more than half the votes in their favour from these commissioners [16].

2. **Miner**: - These nodes will be responsible for adding blocks to the blockchain. The commissioner will choose them on the basis of their reputation (based on their previous work). They will form a block out of all the floating transactions and sign

the block. If the block is validated successfully and no malicious activity is discovered, this node will be given points, and its reputation will be increased by the commissioners. Becoming a miner will be a two-step process that involves becoming a miner candidate and then winning the election for the miner. Re-election will take place after the expiration of their term of office.

3. **Miner candidate**: - As the number of miner nodes is fixed, the other registered nodes act as miner candidates that are given special work. As mentioned before, the miner candidates will be given authority to investigate the FIR transactions, which will be given to them by the commissioner nodes via elections, and hence they will provide the client with updates about the case. The transaction will be signed by their digital signatures so that if they fail to fulfil all the clauses mentioned in the smart contract, they are identified, and their reputation is decreased. Also, if this happens, the information will be transferred to another miner candidate. They are eligible to be a miner only if elected by the commissioner nodes.

4. **Client**: - All of the four roles use the digital signature to authenticate their identities. They need to sign the messages they send so that their actions be verified easily. Ordinary users can join or leave the blockchain network anytime without being authorized, and their behaviour can be arbitrary. They will need to have an account on the mobile application in order to add a FIRs in their name. They will only participate in the public part of the blockchain and can only take part in the process of making transactions of their FIR and mentioning additional clauses of smart contracts if any.

4 Proof of Vote

4.1 Consensus Process

The algorithm that we will use for consensus is proof of voting. The assumptions in this algorithm require that there be N_c total commissioners, N_m miners, N_{mc} miner candidates and N_{cl} clients. Let the total number of nodes be N_{all}. Where $N_{all} = N_c + N_m + N_{mc} + N_{cl}$. For our algorithm, we consider one cycle to be composed of several rounds of consensus, each producing one block. The cycle gets over when a certain number of blocks are mined by the miners, say B, and one extra block pertaining to the elections, its results and the server information of the newly elected miners (as part of the Proof of Vote mechanism) get approved and added in the blockchain. The complete cycle thus generates a total of $B + 1$ blocks at the end of it and is termed as a tenure cycle. The duration of the tenure cycle is T_t. This is also the duration of completion of a miner's tenure. Let there be a random number assigned to each miner, from 0 to $N_m - 1$ and let the time period allotted to each miner within which he should mine a block be T_b. The end of each round of consensus produces a valid block, signed and approved by at least $N_c / 2 + 1$ i.e.,

51% of the commissioners [17]. After generating a block, if the block gets validated, the miner calls for a function that generates a random number R between (0, N_m), which is matched with another miner having the same number. Now, this miner is the one who performs the next round of consensus and takes the procedure forward. If the block does not get validated, it must have happened because of one of the following two reasons:
The miner might have exceeded the time within which he was required to mine the block, i.e., T_b.
In such situations, the task of mining the block gets passed onto the subsequent miner, i.e., one with the number $R = R + 1$. If this pattern follows and R exceeds N_m, the procedure starts from $R = 0$. It finally reaches consensus when, at least and at most, one block gets validated. Such a procedure of consensus reaches consensus finality.
The miner candidates that are producing the updates and floating transactions can act maliciously and make wrong updates that will cause the commissioner to invalidate the block.
In this situation, the commissioner will delete the invalid transaction of the block. Decrypting the digital signature and finding out the exact person who has floated the malicious transaction, the commissioner can reduce the rewards and scores associated with that police officer's name in their vote-list and appoint some other police officer (miner candidate) to perform further updates on the case. The task of mining, however, is allotted to the same miner again, i.e., a miner with the number R.

After generating the required B number of blocks, the last round of consensus for that tenure runs to produce the special block. In this round, the miner candidates who were till now responsible only for floating transactions with updates will now be competing in elections to be a part of the next lot of miners. Each commissioner will give a vote-list of their own, containing scores of the miner candidates. In the end, topmost N_m contenders will win the election and form the group for carrying out the new round of tenure. The last block will contain the result of the election and related information. This ends one tenure cycle at the completion of which $B+1$ rounds of consensus have already taken place, increasing the blockchain by $B+1$ blocks.

4.2 The Generation of A Valid Block

One round of consensus may take C cycles before a block actually gets validated and added to the chain. Let C_1 be the number of cycles that fail due to the maliciously added transactions and C_2 be the number of cycles that fail due to the inability of a miner to generate the block within the given time restraint (T_b). Thus, the total no of cycles $C = C_1 + C_2$. This means there have been $C - 1$ invalid blocks that have already been rejected. Therefore, the total time for one round of consensus comes out to be $T_r = C * T_b$, where C is equal to $C_1 + C_2$ and ($1 \leq C_2 \leq N_m$). (C_2 causes the

authority of mining to be passed onto the next miner whereas C_1 reauthorizes the same miner for the mining task).

1. In our model, the transactions that will be floating are the FIR made by the users attached with a smart contract and the updates made by the policeman (miner candidates) corresponding to some FIR number. Anybody floating a transaction should have their digital signature attached to it.
2. The unconfirmed FIR gets stored in the transaction pool.
3. As soon as a transaction containing an FIR floats from a user, the commissioner on that network (the network of the police station where FIR was filed) appoints a miner candidate who will handle the case by sending him a message on the app.
4. The transactions containing the FIR will be picked up by the appointed police officer (miner candidates) who will work on the case and float an update within the time specified in the smart contract (T_{sc}) failing which will affect their rewards and reputation.
5. The transactions containing the updates will be picked up by a miner numbered i where $i = R$ and R is the random number of the previous block. For the addition of the genesis block, the value of R is zero by default.
6. These transactions are packed into one block and sent to all the commissioners. If a commissioner verifies a block, he signs the block header and sends it back.
7. The cut-off time for this block is T_{cutoff} = time for the previous block to get confirmed + T_b.
8. If the miner receives at least $N_c / 2 + 1$ signed blocks back within T_{cutoff}, he can add the random number of the block and his own signature and finally add it to the blockchain.
9. After T_{cutoff} though, the block becomes invalid and $R = R+1$ as discussed in section 4.1
10. If the block gets rejected due to some malicious actions, follow the procedure described in section 4.1.
11. In either case, however, the time between the addition of two blocks i.e., passing of an update by the police station to the client, should not exceed T_{sc} as per the terms of the contract. If this happens, the miner or the miner candidate whosoever is responsible shall have their reputation on the vote-list at stake.
12. If $C \geq N_b$, this will imply that none of the miner presents could actually mine a valid block, and now C will equate to 1 again. If this continues to happen, the network may fall into a dead circle.

5 Numerical Analysis

In this section, we perform some simulations to test, verify, and compare the effectiveness of the proposed model with the current system. Fig. 3 shows a plot between Incentive ($ per case) and the number of cases solved. In the current system, there is no per case incentive or a bonus for the officers. Therefore, a lack

of motivation is observed among the officers to pick more cases. In the proposed model, the officers are allowed to become the miners based on the efficiency they show in solving the cases. Therefore the officers are more motivated to pick more cases and solve them in as little time as possible. Therefore, the figure shows exponential growth in terms of Incentive earned by the officers in the proposed model. The growth in Incentive is very slow and linear in the current system, as shown in the figure. Fig. 4 shows a plot between the average time at solving each case (months) and the number of FIRs registered. In the current system, as more FIR gets registered, it will increase the time to solve the individual case. Whereas in our proposed model, police officers will get Incentive when they successfully solve the case. This will motivate the police officers to solve the cases correctly and quickly. Therefore the average time will decrease exponentially as the number of FIRs increases.

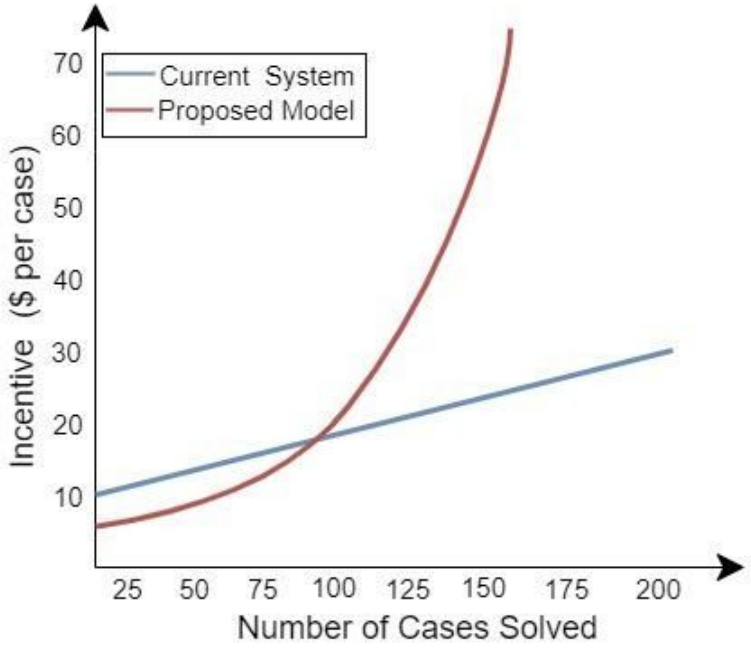

Fig. 3. Comparison of growth of Incentive for the officers solving the FIR cases.

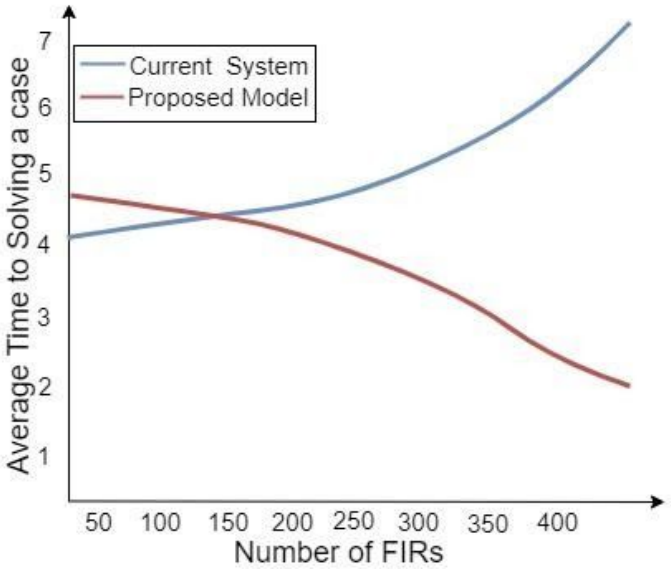

Fig. 4. Comparison of Average time to solve a case (Months) with the increasing number of FIRs.

6 Conclusion

The conventional method is prone to delays and inefficiency. This paper proposes to simplify and speed up the process of FIR registration and tracking through the use of consortium blockchain technology. We presented the complete consensus process using the Proof of Vote protocol. We designed four identities for network participants based on the key idea of the voting mechanism. This guarantees the separation of voting and execution rights that enhance the independence of miner's role, so does the internal control system within the consortium. With the advancement of Information and Communication Technology, our proposed method will definitely boost up the FIR proceedings. Therefore this paper aims to help the citizens and the police officials alike. The proposed system would guarantee the acceptance and response of the FIRs from the police department to the complainants. Thus, the ease of access, registry, and tracking will encourage a more judicial and lawful society.

References

1. Wolfie Zhao, "Dubai Plans to 'Disrupt' Its Own Legal System with Blockchain," https://www.coindesk.com/dubai-plans-to-disrupt-its-own-legalsystem-with-blockchain , online; accessed 11 March 2019.
2. Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful

incentive mechanism for distributed p2p applications," IEEE Access, vol. 6, pp. 27 324–27 335, 2018.
3. S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "Pbcert: Privacy-preserving blockchain-based certificate status validation toward mass storage management," IEEE Access, vol. 7, pp. 6117–6128, 2019.
4. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," IEEE transactions on industrial informatics, vol. 14, no. 8, pp. 3690–3700, 2018.
5. T. Alladi, V. Chamola, and K. Choo, "Consumer IoT: Security vulnerability case studies and solutions," IEEE Consumer Electronics (Sep 2019), 2019.
6. T. Alladi, V. Chamola, and J. Rodrigues, "Blockchain in smart grids: A review on different use cases," Sensors, MDPI, 2019.
7. N. Fabiano, "Internet of things and blockchain: legal issues and privacy. the challenge for a privacy standard," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017, pp. 727–734.
8. G. Bansal, V. Hassija, V. Chamola, N. Kumar, and M. Guizani, "Smart stock exchange market: A secure predictive decentralised model," in IEEE Globecom, Waikoloa, USA, Dec. 2019, Dec 2019, pp. 1–6.
9. C. Sillaber and B. Waltl, "Life cycle of smart contracts in blockchain ecosystems," Datenschutz und Datensicherheit-DuD, vol. 41, no. 8, pp. 497–500, 2017.
10. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, 2019.
11. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.
12. C. Cachin and M. Vukoli´c, "Blockchain consensus protocols in the wild," arXiv preprint arXiv:1707.01873, 2017.
13. Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," Work Pap.–2016, 2016.
14. I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." IJ Network Security, vol. 19, no. 5, pp. 653–659, 2017.
15. V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops), May 2019, pp. 1–6.
16. V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," Computer Communications, 2019.
17. V. Hassija, M. Zaid, G. Singh, A. Srivastava, and V. Saxena, "Cryptober: A blockchain-based secure and cost-optimal car rental platform."