INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

R&D SHOWCASE 2021

E-Governance and Information Aggregation over Blockchains

Secure E-Governnace

Auctions

- **Aim**: Maximize Social Welfare
- Combinatorial auctions generate greater revenue
- How to get agents to elicit their true valuation?
- How to protect the privacy of these bidding information?
- **Our Approach:** Yao's Millionaires' Problem
  - Secure Comparison of two integers [4]

Voting

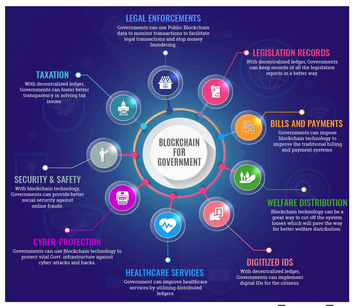
- **Aim:** Fair Voting System
- Voting requires high levels of anonymity, privacy and security
- In addition to this, the votes should be immutable and verifiable

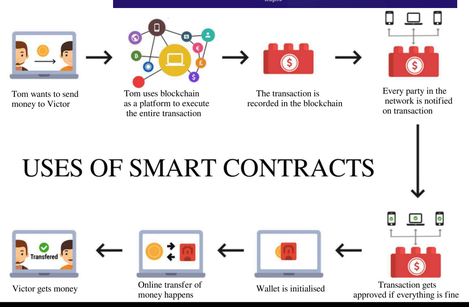
Record Management

- **Aim**: Secure maintenance of data
- Is it safe to have trust in a single party?
- How to assure that the data is not lost?

Solution: Smart Contracts

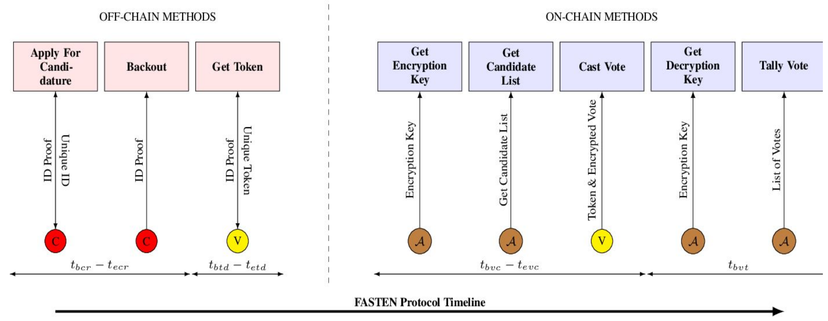
- Use of **Smart Contracts** is the main advantage of Blockchain Technology in **e-governance.**
- Decentralisation, Data integrity, Transparency: **Increased effectiveness** of government.
- **Convenient** means of interaction between citizens and government





FASTEN: Fair and Secure Distributed Voting Using Smart Contracts [1]

- **Voter Anonymity:** A vote cannot be traced back to the voter
- **Vote Concealment:** The vote's value should remain hidden from the system
- **Vote Immutable**: A vote should be impossible to alter by anyone
- **Double Voting Inhibition:** A voter should be allowed to vote only once in a specific election



PUBLICATIONS

1. Sankarshan Damle, Sujit Gujar, & Moin Hussain Moti (2021). FASTEN: Fair and Secure Distributed Voting Using Smart Contracts. **ICBC**, 2021.
2. Moin Hussain Moti, Dimitris Chatzopoulos, Pan Hui, Boi Faltings, Sujit Gujar. (2020). Orthos: A Trustworthy AI Framework for Data Acquisition. **EMAS,** 2020.
3. Moin Hussain Moti, Dimitris Chatzopoulos, Pan Hui, Sujit Gujar. (2019). FaRM: Fair Reward Mechanism for Information Aggregation in Spontaneous Localized Settings. **IJCAI,** 2019.
4. Sankarshan Damle, Boi Falting & Sujit Gujar. (2019). A Truthful, Privacy-Preserving, Approximately Efficient Combinatorial Auction For Single-minded Bidders. **AAMAS,** 2019.
5. Dimitris Chatzopoulos, Sujit Gujar, Boi Faltings, & Pan Hui. (2018). Privacy Preserving and Cost Optimal Mobile Crowdsensing Using Smart Contracts on Blockchain. IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems **MASS,** 2018.

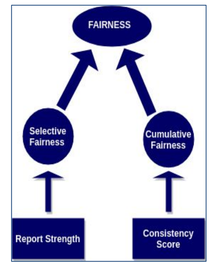
Information Aggregation

Crowdsourcing

- **Example**
  - NASA's Space Robotics Challenge
  - DARPA Red Balloon Challenge
  - Mobile Crowdsensing [5]
- **Challenges**
  - Information Elicitation
  - Ensuring Privacy
  - Fair Rewards

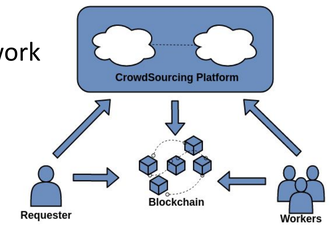
FARM: Fair Reward Mechanism [3]

- **Nash Incentive Compatible** Mechanism
- Spontaneous localized settings
- Fair reward is acheived from:
  - **Selective Fairness:** Agents with same reports are evaluated similarly
  - **Cummulative Fairness:** Considers agent's consistency and history of reporting as part of reward
- **Reward** considers the following scores:
  - Report Strength
  - Consistency Score
  - Reliability Score
  - Location robustness Score



ORTHOS: A Trustworthy AI Framework For Data Acquisition [2]

- Blockchain-based trustworthy framework for **spontaneous location-based** information aggregation



Affiliate: *Dr. Sujit P. Gujar, Samhita Kanaparthy, Sankarshan Damle*

Research Center: Machine Learning Lab