

## 2018 Research Interest/Project Ideas

**Dr. Aniket Kate**

<https://freedom.cs.purdue.edu/blockchains>

Potential projects: Today's geo-politically distributed organizations and consortia are faced with an acute demand for transparency. While the blockchain technology has the potential to meet this demand, the current blockchain frameworks are not private, flexible, and scalable enough to solve the hard transparency/provenance problems in the industry. Over the last three years, My students and I have been actively enhancing blockchains to make those useful for distributed organizations & consortia. Our prominent ongoing and near-term research and development projects are as follows:

---

### **Enabling Access Control and Revocations in 'Immutable' Blockchain Ledgers**

The use of the existing Blockchain technologies may negatively affect privacy in several distributed application scenarios. We are developing cryptographic solutions towards enforcing any monotonous access control on blockchain ledgers. In the near future, we also plan to address the inherently hard problem of access revocation, which becomes even harder for blockchains as they are immutable by nature.

---

Our other on going blockchain projects include

- \* Protecting Privacy for Smart Contract (i.e., Business Logic) from Prying Eyes, and
- \* Crypto-augmented Smart Contracts for Solving Problem that cannot be solved blockchains and cryptography alone.

Our work has been supported by National Science Foundation, Northrop Grumman, Ford Motors, Intel, and the German Universities Excellence Initiative.