Economics of Privacy, Blockchain and Trust

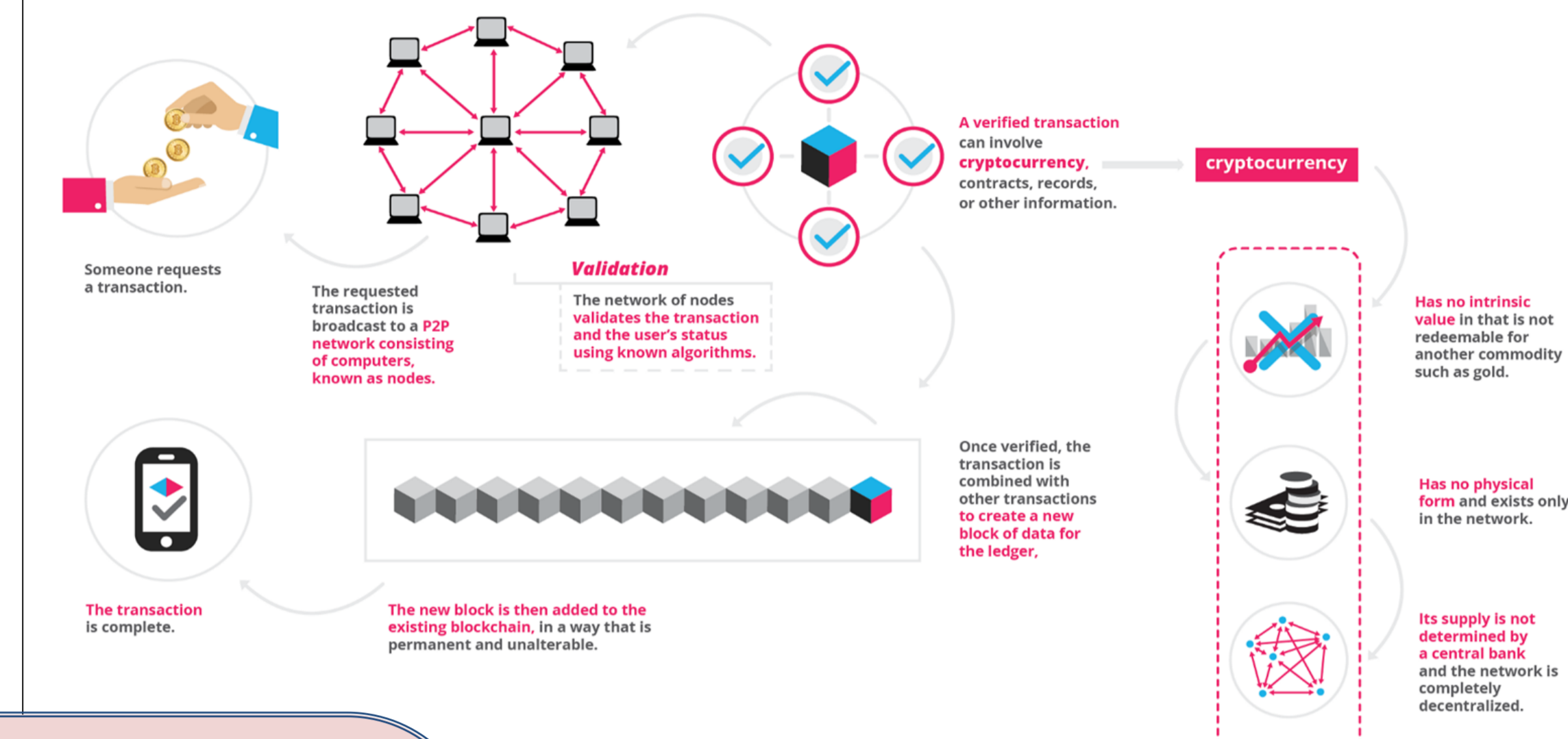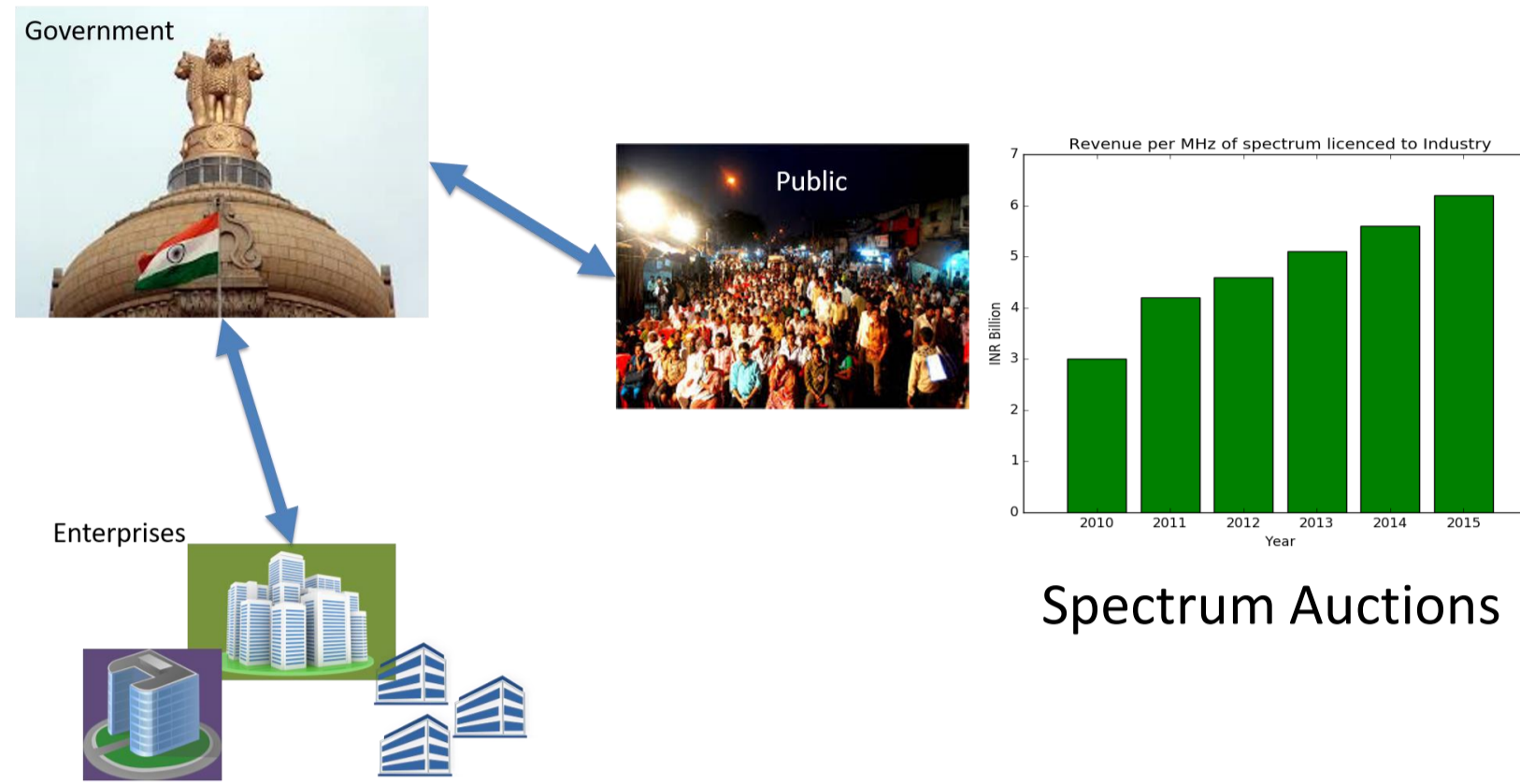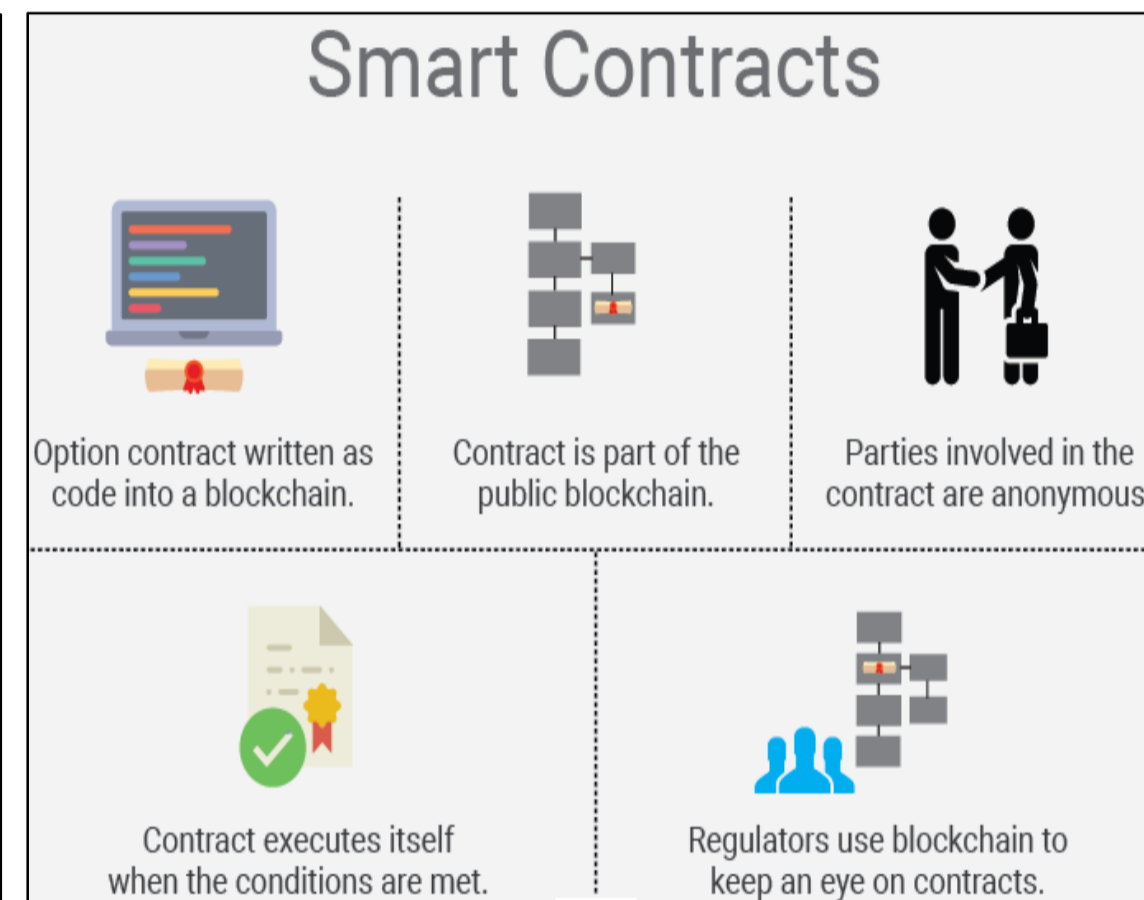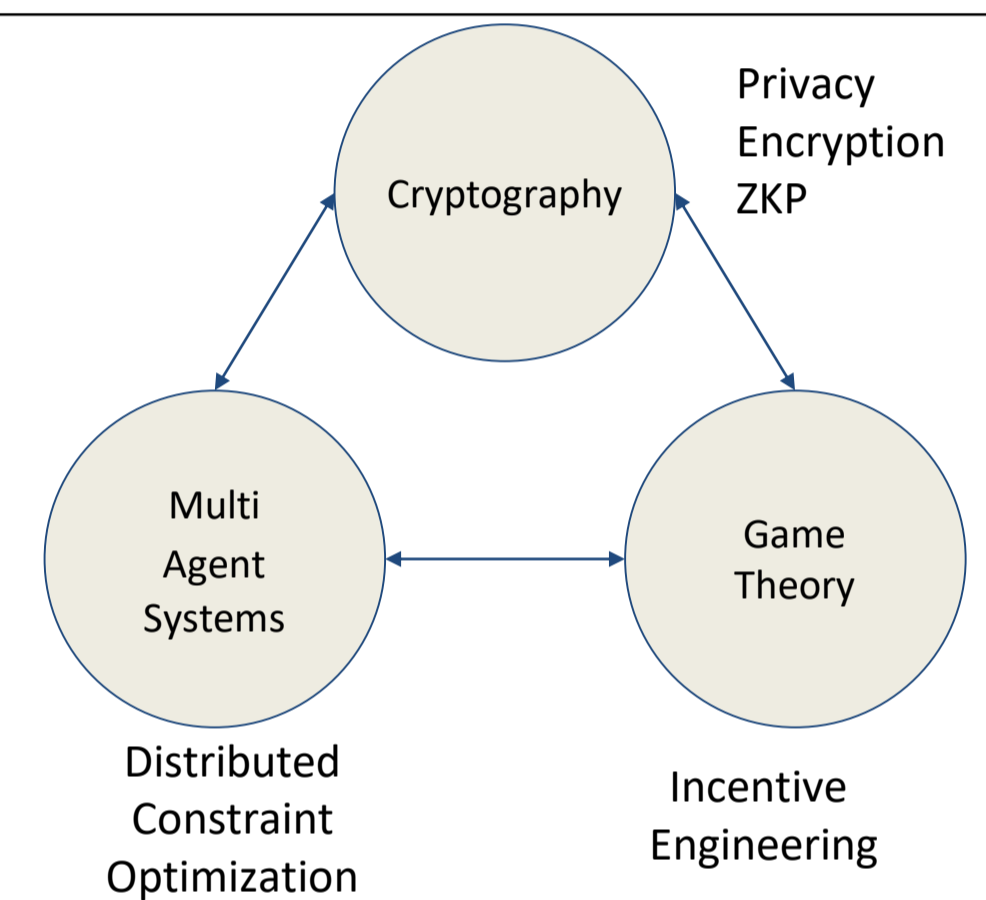INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Auctions

- Goal: Maximize **Social Welfare**
- Combinatorial auctions generate greater revenue
- How to ensure that agents elicit their **true valuation**?
- How to protect the **privacy** of these bidding information?

Government

Public

Enterprises

Spectrum Auctions

Cryptography

Privacy Encryption ZKP

Multi Agent Systems

Game Theory

Distributed Constraint Optimization

Incentive Engineering

Smart Contracts

Option contract written as code into a blockchain.

Contract is part of the public blockchain.

Parties involved in the contract are anonymous.

Contract executes itself when the conditions are met.

Regulators use blockchain to keep an eye on contracts.

Objectives

- How to improve privacy in blockchain technology; Proof of Location
- How to design appropriate incentives for making blockchain sustainable
- How to design new verifiable, game theoretic mechanisms that preserve privacy, e.g. Auctions, Voting
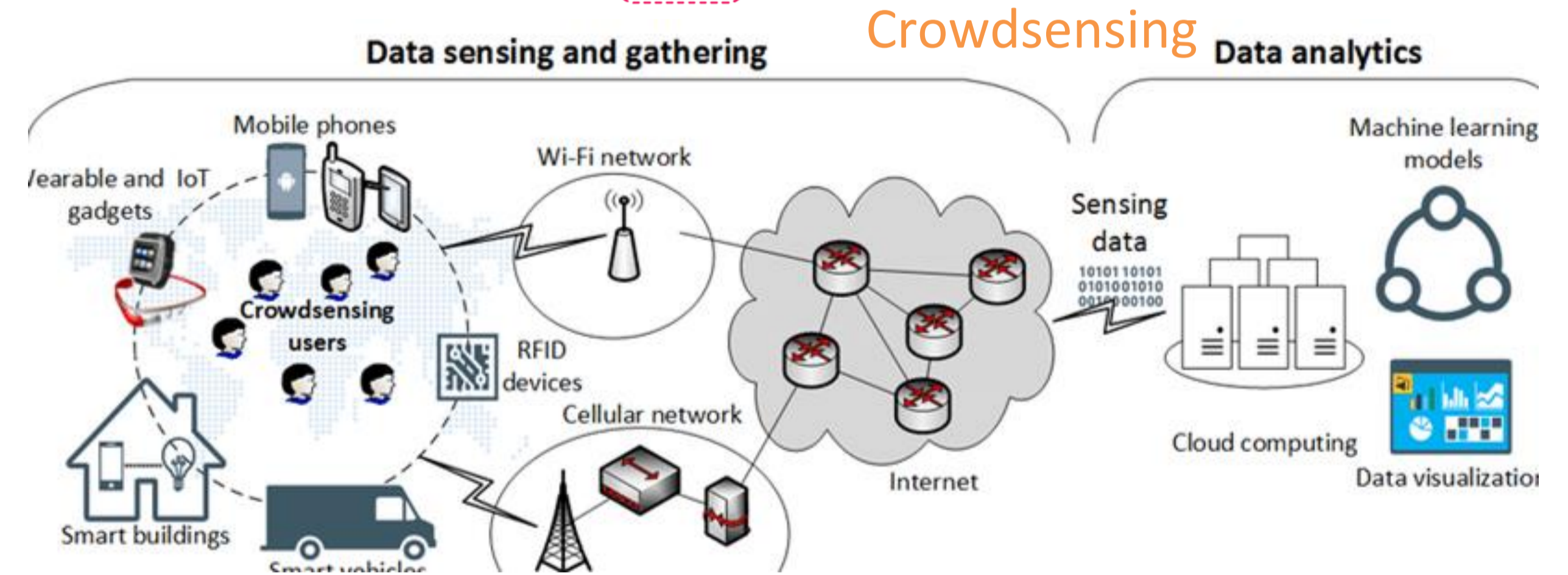
Challenges

- How to operate on encrypted data?
  - Homomorphic Encryption
    - allows complex mathematical operations to be performed on encrypted data
    - commitment functions
- How to eliminate centralized third party?
  - Secure Multi-Party Computation
    - formulate as DCOPs
    - smart contracts

Bidder_2   Bidder_3

b2   b3

Bidder_1

b1

Bidder_0

b0

Method: PDPOP: A solver for DCOP instances

1. Decrypt
2. Compute

Auctioneer

price

Method: Using commitment functions and PKI

Blockchains

A verified transaction can involve **cryptocurrency**, contracts, records, or other information.

Someone requests a transaction.

The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.

Validation The network of nodes validates the transaction and the user's status using known algorithms.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,

The transaction is complete.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

- Blockchain is an ideal platform for **secure** and **anonymous decentralized** applications
- It relies on the fact that majority of users are honest, that is **trust** is **distributed** in the network than on one node
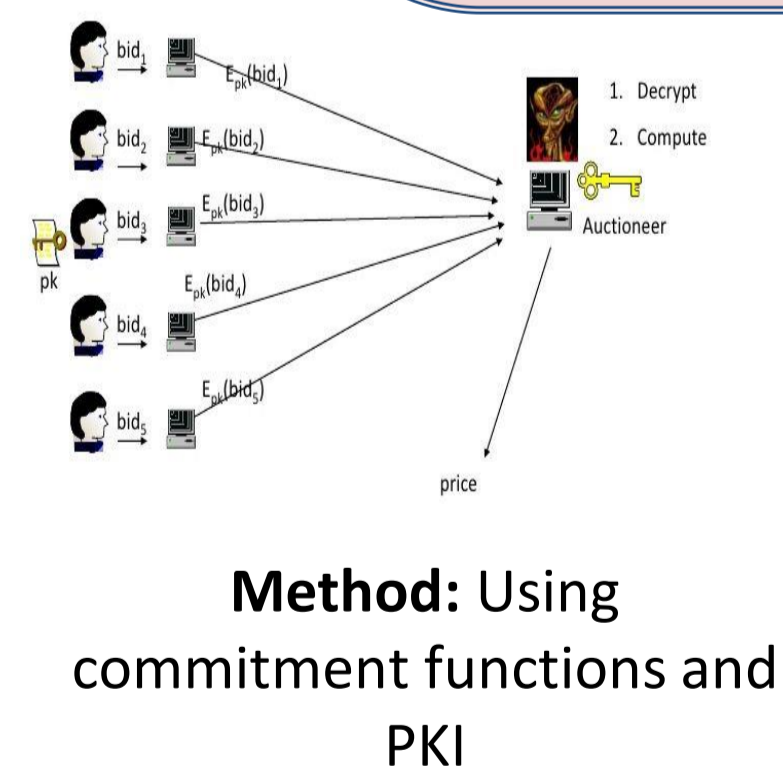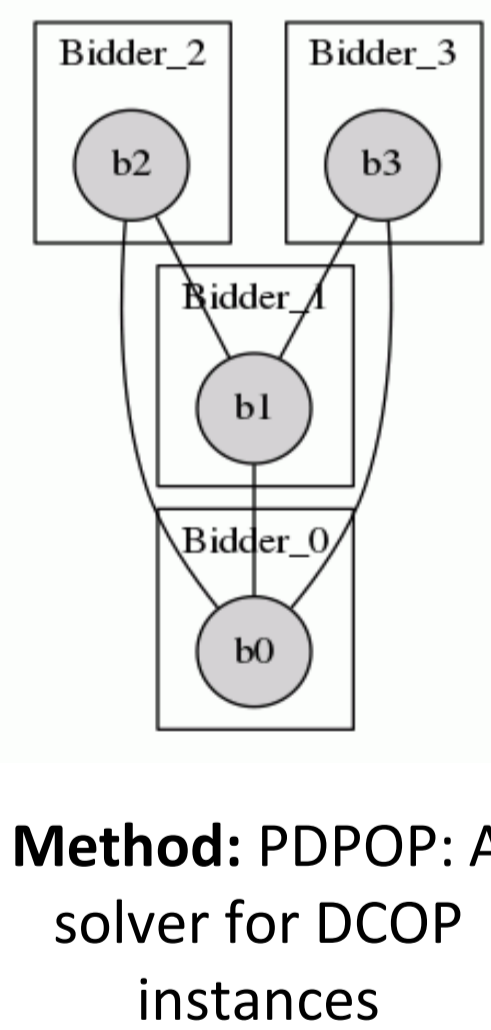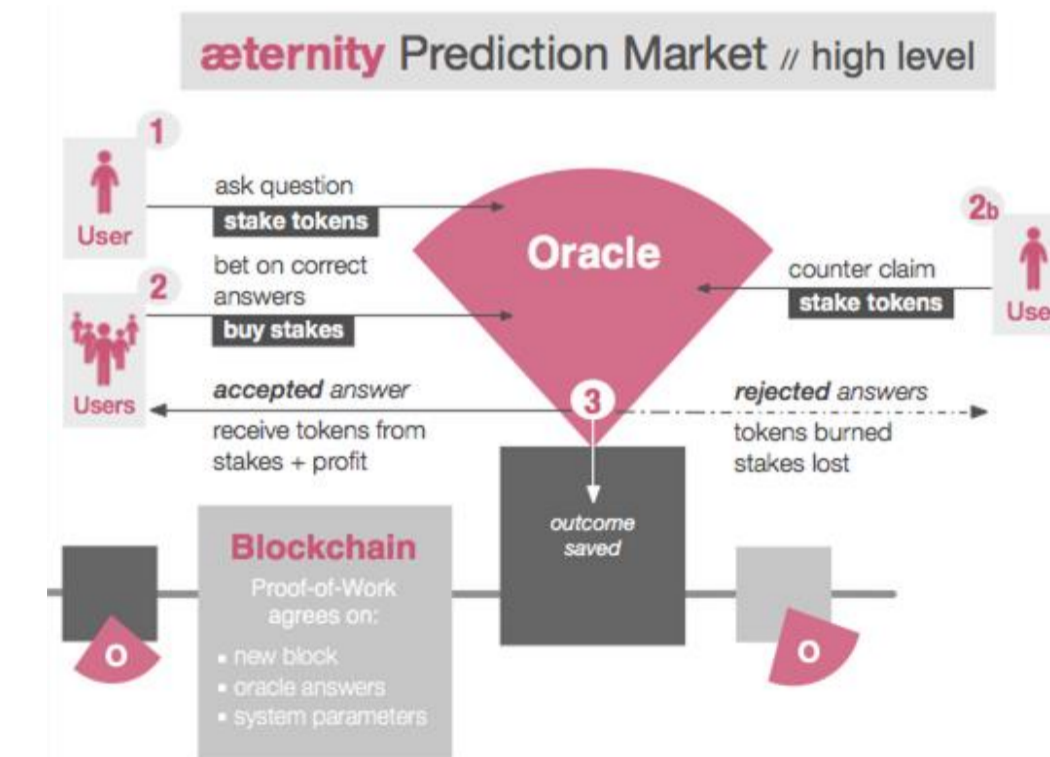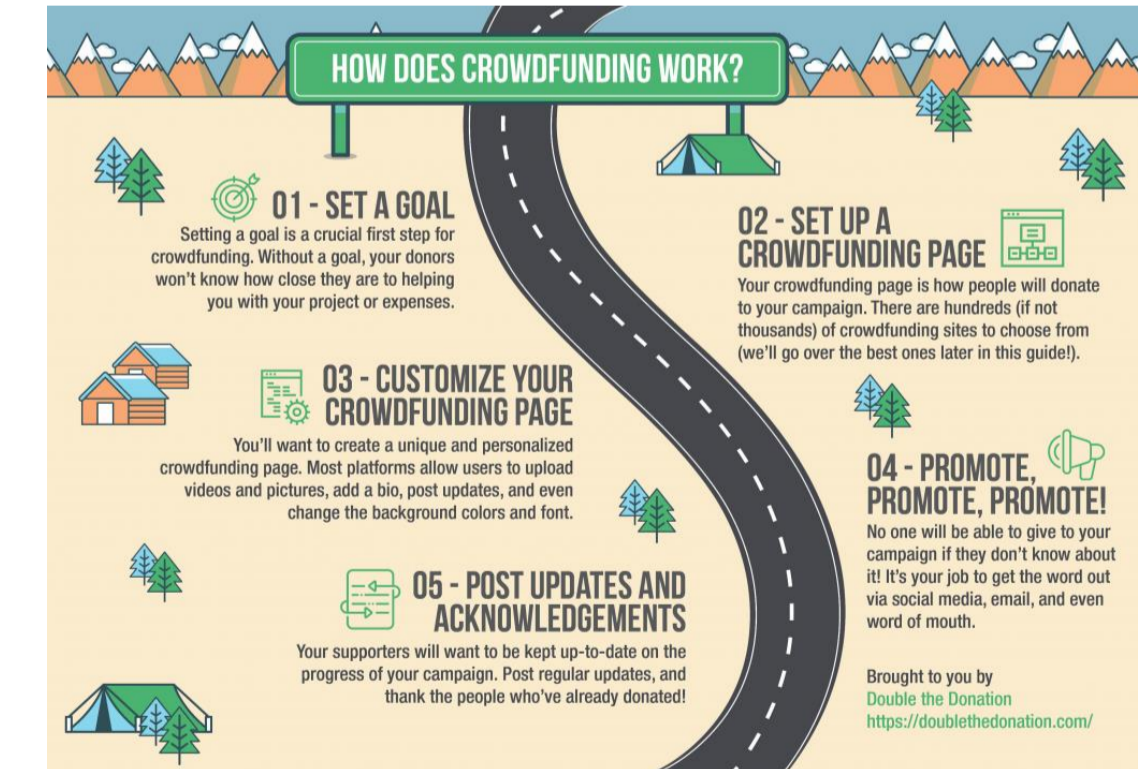
Crowdsensing

Data sensing and gathering   Data analytics

Mobile phones   Wi-Fi network   Machine learning models

Wearable and IoT gadgets   Sensing data

Crowdsensing users   RFID devices   Cellular network   Cloud computing

Smart buildings   Smart vehicles   Internet   Data visualization

Voting

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

Prediction Markets

æternity Prediction Market // high level

1. User   ask question stake tokens

bet on correct answers buy stakes

2a. User   counter claim stake tokens

Oracle

accepted answer   rejected answers

receive tokens from stakes + profit   tokens burned stakes lost

3   outcome saved

Blockchain Proof-of-Work agrees on:
- new block
- oracle answers
- system parameters

Crowdfunding

HOW DOES CROWDFUNDING WORK?

01 - SET A GOAL
Setting a goal is a crucial first step for crowdfunding. Without a goal, your donors won't know how close they are to helping you with your project or expenses.

02 - SET UP A CROWDFUNDING PAGE
Your crowdfunding page is how people will donate to your campaign. There are hundreds (if not thousands) of crowdfunding sites to choose from (we'll go over the best ones later in this guide!).

03 - CUSTOMIZE YOUR CROWDFUNDING PAGE
You'll want to create a unique and personalized crowdfunding page. Most platforms allow users to upload videos and pictures, add a bio, post updates, and even change the background colors and font.

04 - PROMOTE, PROMOTE, PROMOTE!
No one will be able to give to your campaign if they don't know about it! It's your job to get the word out via social media, email, and even word of mouth.

05 - POST UPDATES AND ACKNOWLEDGEMENTS
Your supporters will want to be kept up-to-date on the progress of your campaign. Post regular updates, and thank the people who've already donated!

Brought to you by Double the Donation

Publications

- Praphul Chandra, Sujit Gujar and Y. Narahari, "Referral-Embedded Provision Point Mechanisms for Crowdfunding of Public Projects". In the Proceedings of the 2017 International Conference on Autonomous Agents and Multiagent Systems (AAMAS'17).
- Dimitrios Chatzopoulos, Sujit Gujar, Boi Faltings and Pen Hui, "LocalCoin: An Ad-hoc payment scheme for areas with high connectivity". MobiHoc 2016
- Moin Hussian Moti and Sujit Gujar, "DisTVote: Improving Fairness in Elections Through Distributed Trust". Under Review.
- Dimitrios Chatzopoulos, Sujit Gujar, Boi Faltings and Pen Hui, "Privacy Preserving and Cost Optimal Mobile Crowdsensing using Smart Contracts on Blockchain", Under Review.

Moin Hussain Moti, Sankarshan Damle, Sujit Prakash Gujar

Machine Learning Laboratory