SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME: 19CS622-Blockchain Technology

III YEAR /VI SEMESTER

Unit 1- INTRODUCTION TO BLOCKCHAIN

Topic 6: Blockchain structure

Brain Storming

1. Blockchain terminologies
2. Define Distributed ledger.

Types of blockchain

- There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.

✓ Public Blockchain:

no one in charge, anyone can participate in reading/writing/auditing the blockchain (i.e. Bitcoin, Litecoin, etc.)

✓ Private Blockchain:

a private property of an individual or an organization, there is one in charge of important things such as read/write or whom to selectively give access to read or vice versa (i.e. Bankchain)

✓ Consortium or Federated Blockchain:

More than one in charge. A group of companies or representative individuals come together and make decisions for the best benefit of the whole network (i.e. r3, EWF)

Types of blockchain

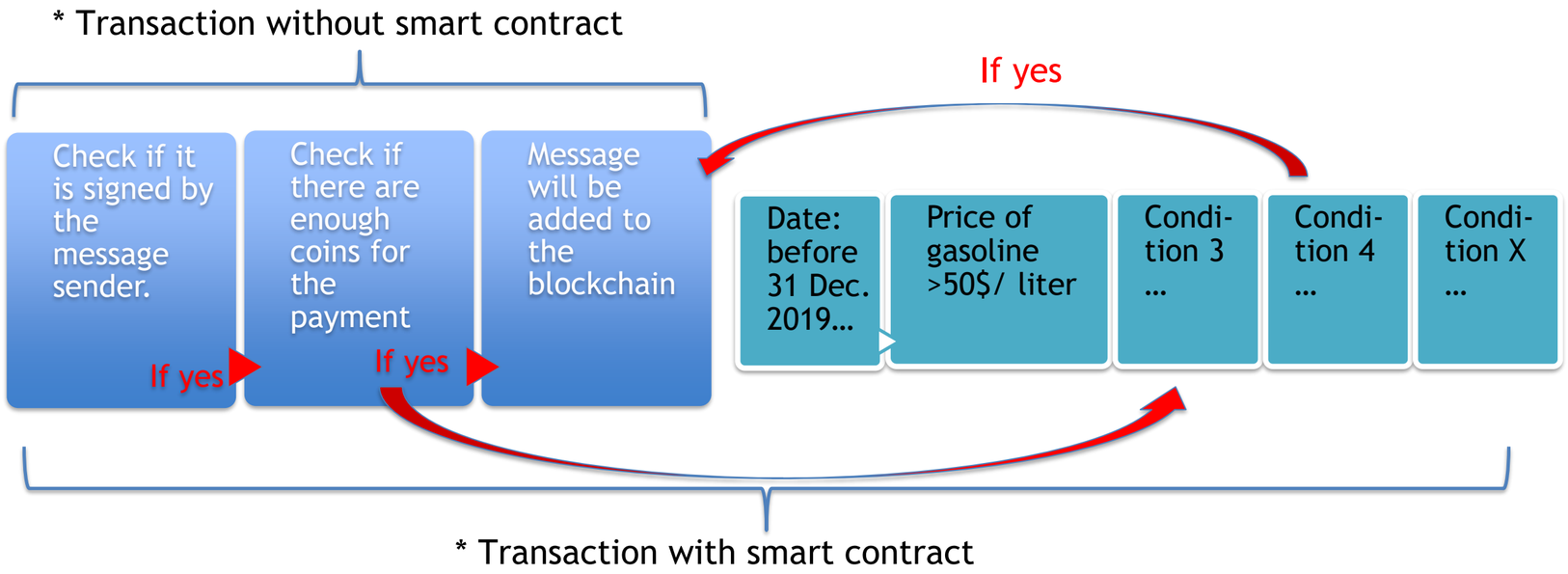
- Smart contract theory
  1. Smart Contract Theory and architecture
  2. Architectures and decentralized autonomous systems
- Smart contract application
  1. Existing blockchain applications, related structures and architectures

Smart Contract Theory and architecture

- **Smart Contract Theory**
  - A computer protocol designed digitally facilitate, verify, or enforce the negotiation or performance of a contract.
  - It allows the performance of credible transactions without the third parties.
  - The transactions are traceable and irreversible.

Consensus components

- **Smart Contract architecture**

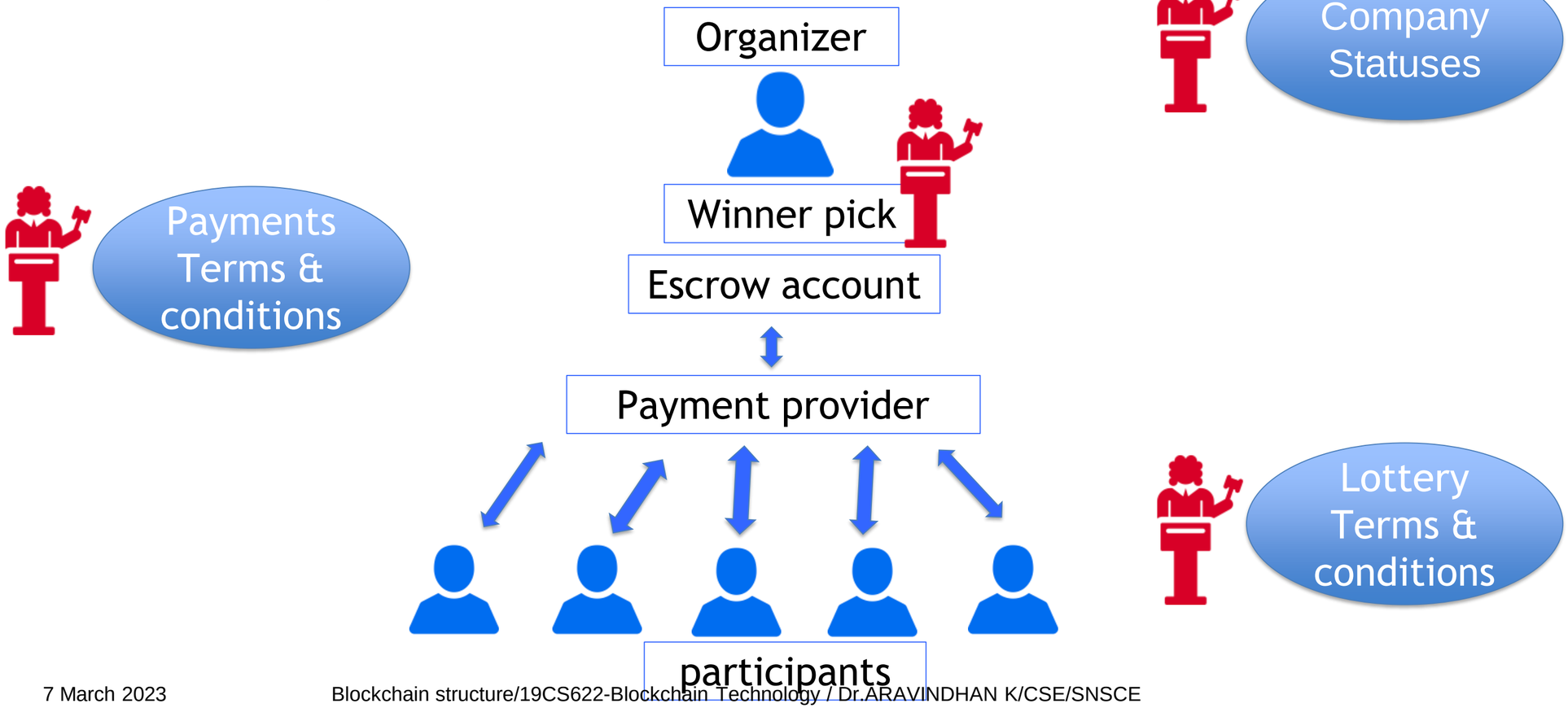


Architectures and decentralized autonomous systems

- **DAO (**Decentralized Autonomous Organization)
  - An organization represented by rules encoded as a computer program, which is transparent, controlled by shareholders and not influenced by a central government.
  - It's notionally like the example for getting funds for a small conference, except that it includes much more. Members buy shares in the DAO and can vote on things according to the number of shares they have. The dreamers have the idea they'll replace Democracy and run entire countries this way.
  - The DAO was the largest crowdfunding in history, having raised over $150m from more than 11,000 enthusiastic members. (ICO)
  - A DAO’s financial transaction record and program rules are maintained on a blockchain.

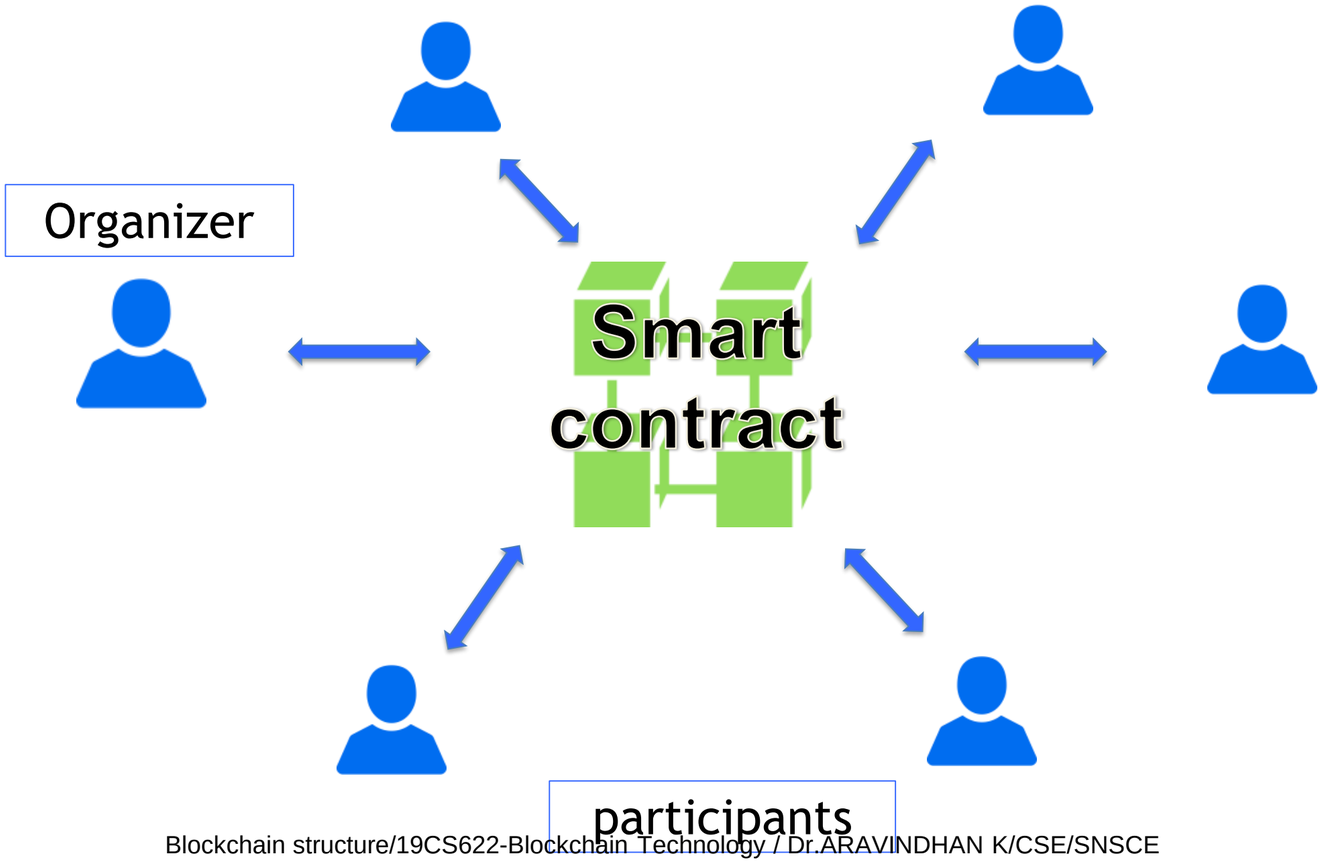
Smart contract application

- **Example 1: Lottery**
  - Lottery without smart contract



Smart contract application

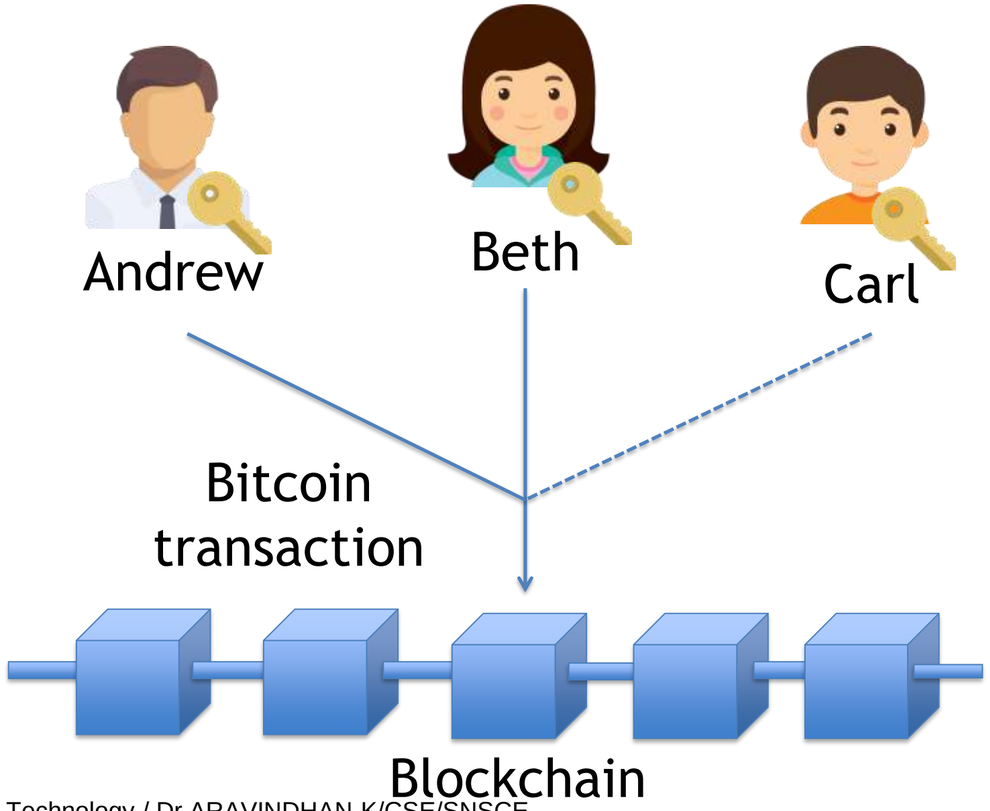
- **Example 1: Lottery**
  - Lottery with smart contract



Smart contract application

- **Example 2-1: Group wallets**
  - Enforcing at least 2 out of 3 people of a group to agree to create a valid transaction

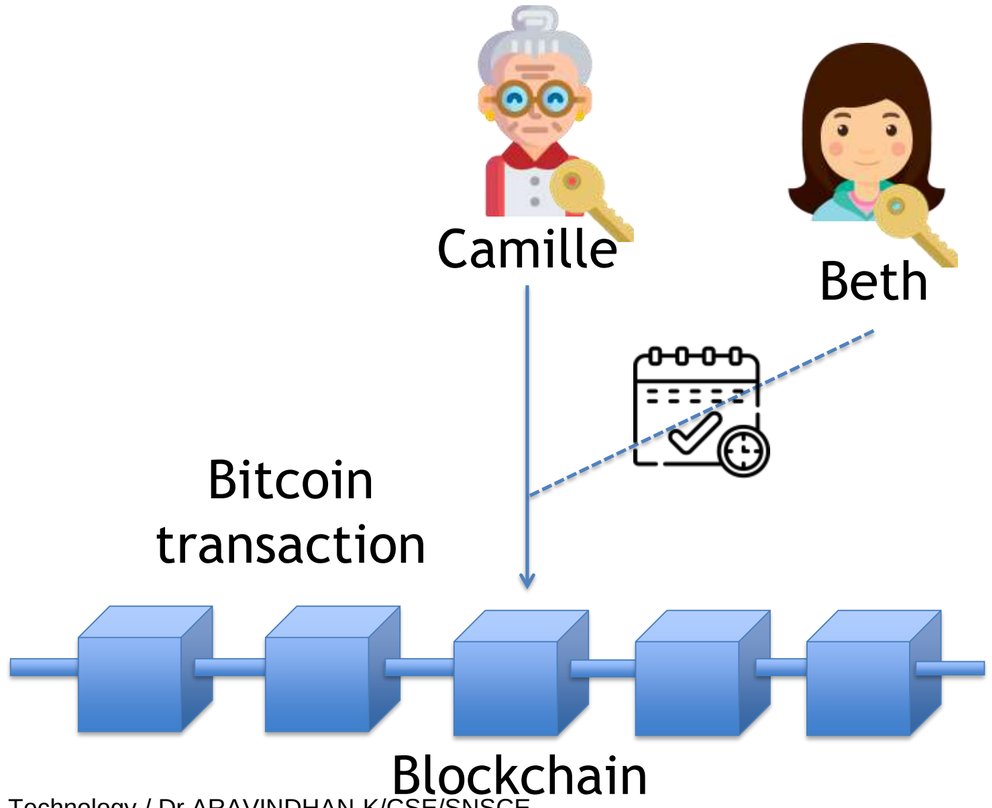
```
2 <pubKeyAndrew>
<pubKeyBeth>
<pubKeyCarl> 3
CHECKMULTISIG
```



Smart contract application

- **Example 2-2: Heritage wallets**
  - Enforcing that a transaction must be signed either by Camille OR by Beth after 5 years

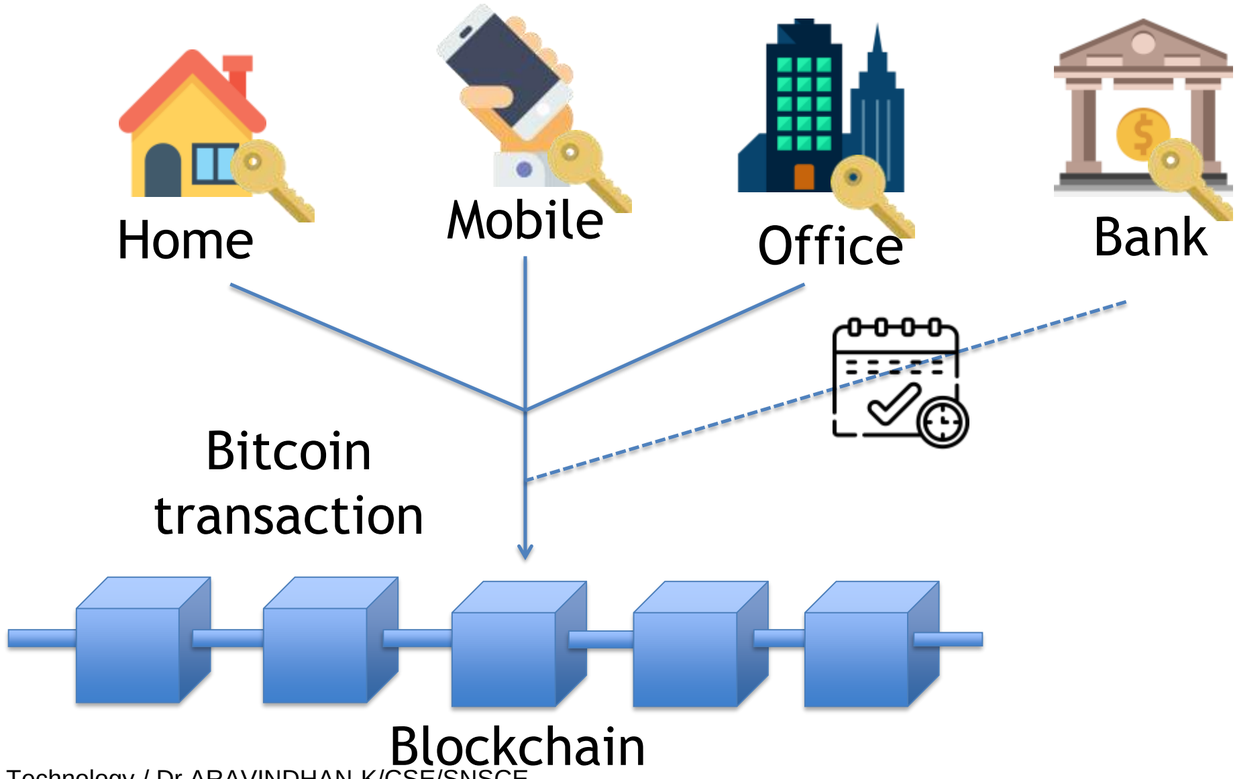
```
IF
   <pubKeyCamille>
   CHECKSIG
ELSE
   <5 y> CLTV DROP
   <pubKeyBeth>
    CHECKSIG
ENDIF
```



Smart contract application

- **Example 2-3: Secure storage**
  - Enforcing that a transaction must be signed by either 3 devices in different locations OR a recovery key deposited in the bank after 8 months

```
IF
        3 <pubKeyHome>
         <pubKeyMobile>
         <pubKeyOffice> OP_3
          CHECKMULTISIG
ELSE
       <8 m> CLTV DROP
       <pubKeyBank>
       CHECKSIG
ENDIF
```



References

TEXT BOOKS

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018
2. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
3. https://101blockchains.com/blockchain-vs-database-the-difference/

REFERENCES

1. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.
2. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming’, Create Space Independent Publishing Platform, 2017.
3. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, July 19, 2016.
4. Henning Diedrich, Ethereum: Block chains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations-2016

Thank You