BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

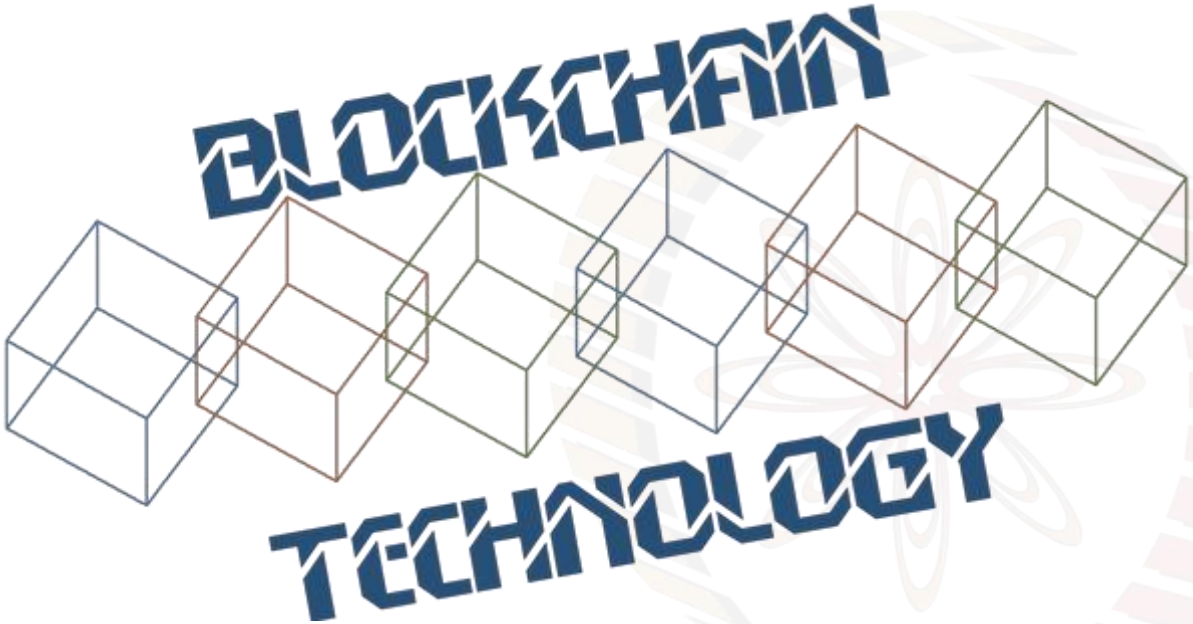
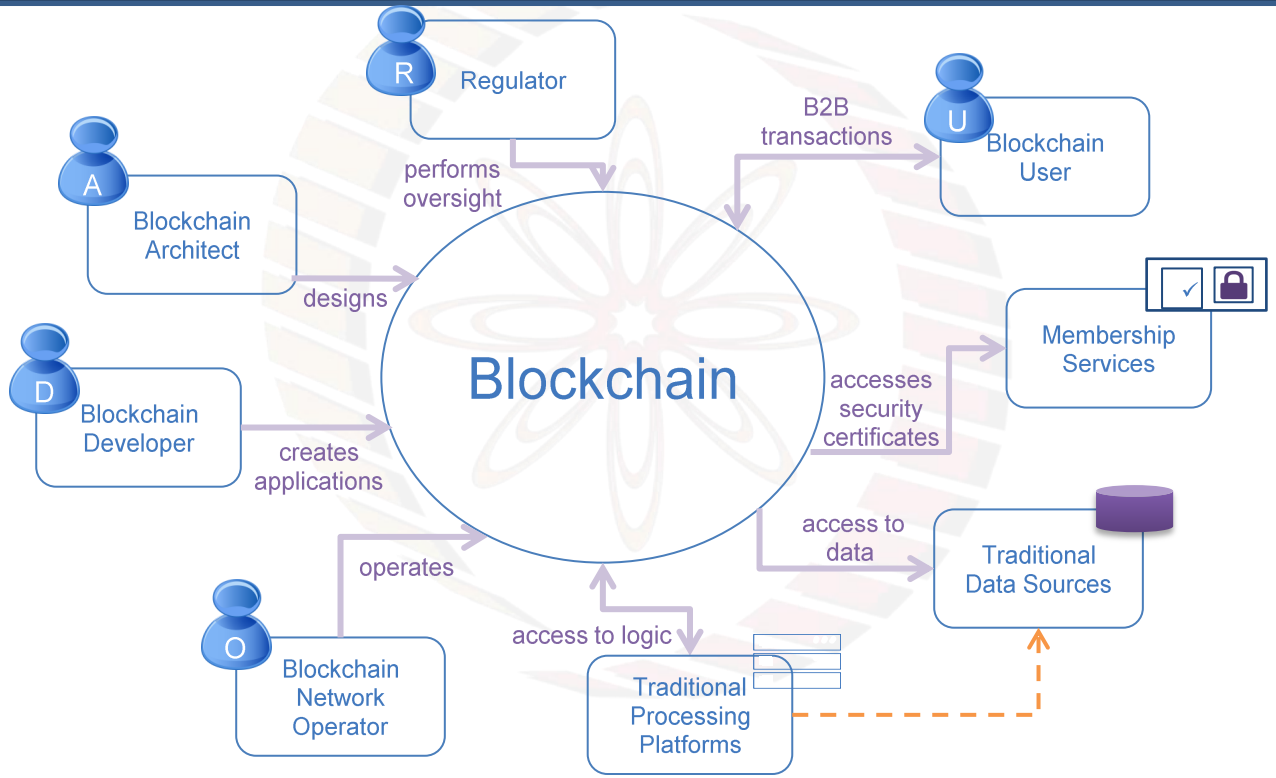


Image courtesy: http://beetfusion.com/

BLOCKCHAIN COMPONENTS AND CONCEPTS

Actors in a Blockchain Solution



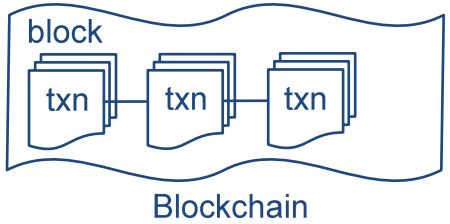
Actors in a Blockchain Solution

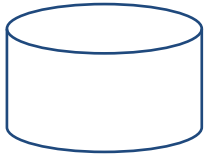
Blockchain Architect	Responsible for the architecture and design of the blockchain solution
Blockchain User	The business user, operating in a business network. This role interacts with the Blockchain using an application. They are not aware of the Blockchain.
Blockchain Regulator	The overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer	The developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Operator	Manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.
Membership Services	Manages the different types of certificates required to run a permissioned Blockchain.
Traditional Processing Platform	An existing computer system which may be used by the Blockchain to augment processing. This system may also need to initiate requests into the Blockchain.
Traditional Data Sources	An existing data system which may provide data to influence the behavior of smart contracts.

Components in a Blockchain Solution

Ledger	A ledger is a channel's chain and current state data which is maintained by each peer on the channel.
Smart Contract	Software running on a ledger, to encode assets and the transaction instructions (business logic) for modifying the assets.
Peer Network	A broader term overarching the entire transactional flow, which serves to generate an agreement on the order and to confirm the correctness of the set of transactions constituting a block.
Membership	Membership Services authenticates, authorizes, and manages identities on a permissioned blockchain network.
Events	Creates notifications of significant operations on the blockchain (e.g. a new block), as well as notifications related to smart contracts.
Systems Management	Provides the ability to create, change and monitor blockchain components
Wallet	Securely manages a user's security credentials
Systems Integration	Responsible for integrating Blockchain bi-directionally with external systems. Not part of blockchain, but used with it.

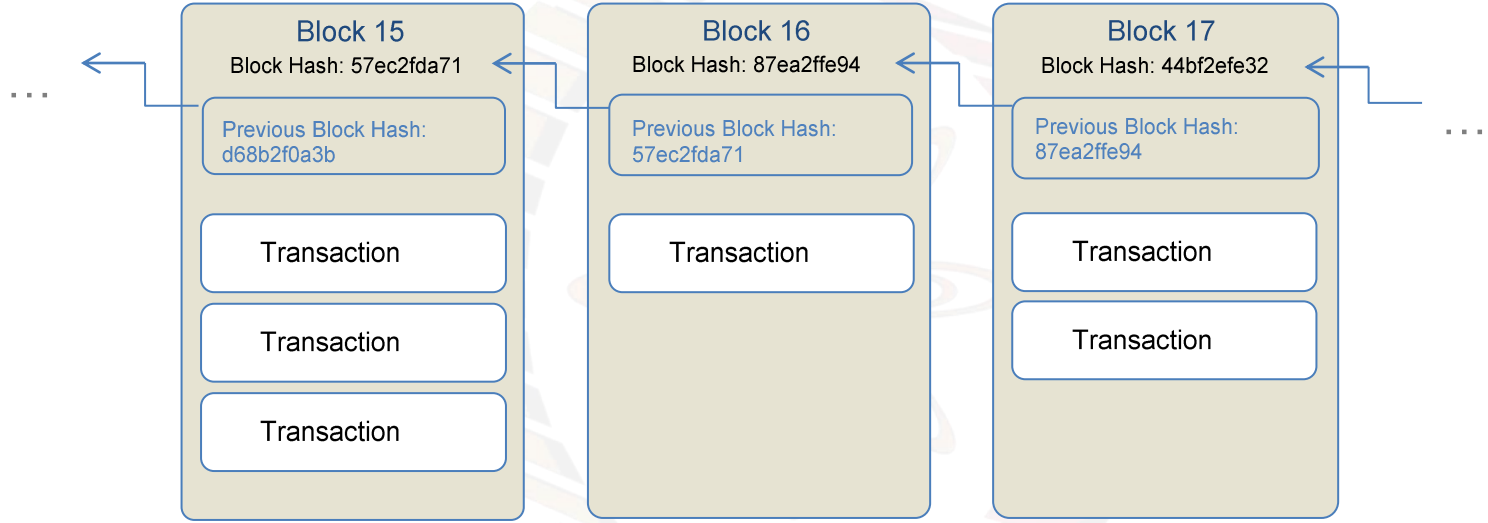
A ledger often consists of two data structures





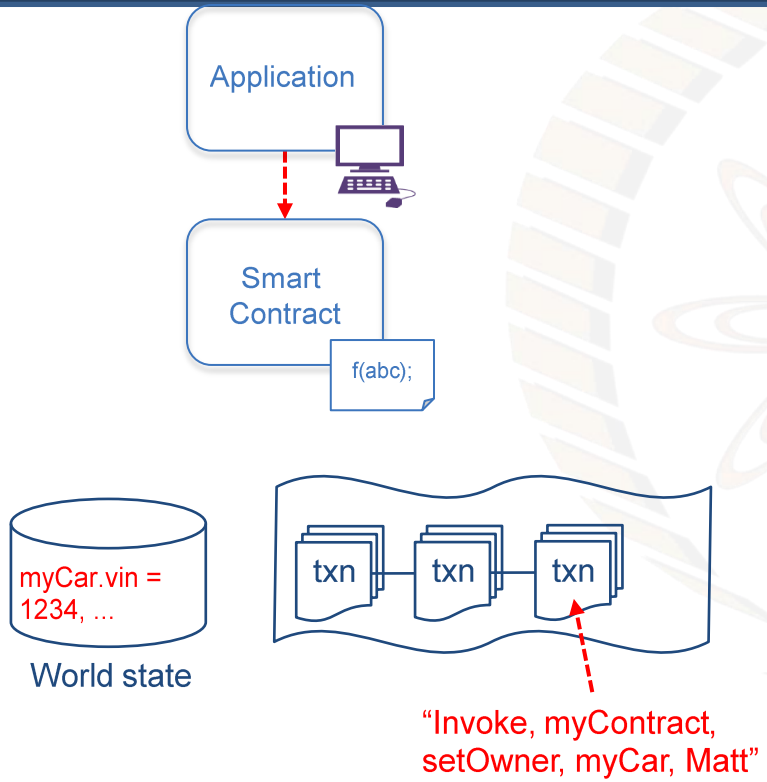
- Blockchain
  - A linked list of blocks (a hashchain)
  - Each block describes a set of transactions (e.g. the inputs to a smart contract invocation, output, identities/certs)
  - Immutable – blocks cannot be tampered
- World State
  - Stores the most recent state of smart contracts / output of transactions
  - Stored in a traditional database (e.g. key-value store)
  - Data elements can been added, modified, deleted, all recorded as transactions on blockchain

Block Detail (Simplified)



- A blockchain is made up of a series of blocks with new blocks always added to the end
- Each block contains zero or more transactions and some additional metadata
- Blocks achieve immutability by including the result of a hash function of the previous block
- The first block is known as the “genesis” block

Ledger Example: A Change of Ownership Transaction



Transaction input - sent from application

```
invoke(myContract, setOwner,
       myCar, Matt)
…
```

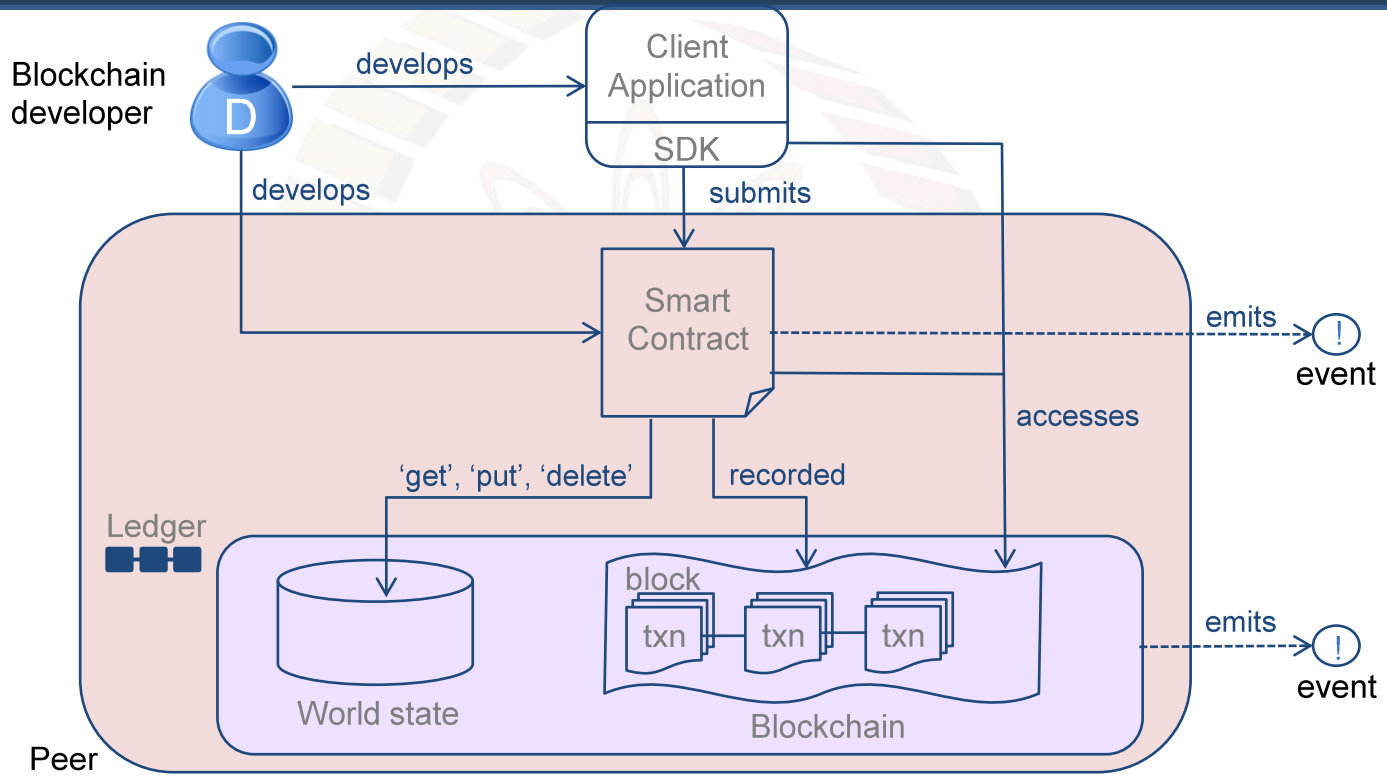
Smart contract implementation

```
setOwner(Car, newOwner) {
  set Car.owner = newOwner
}
```

World state: new contents

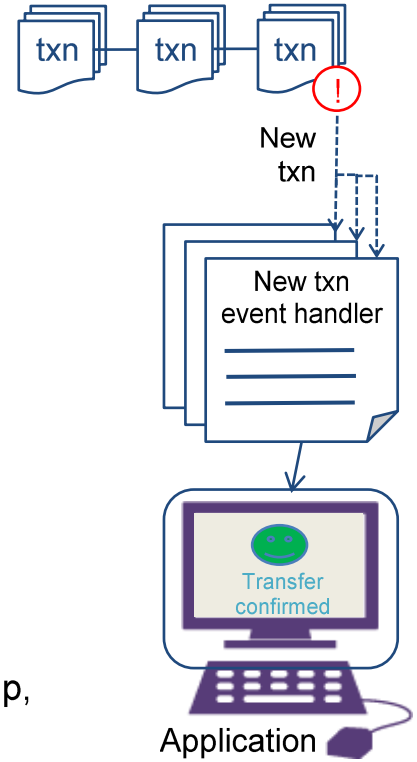
myCar.vin = 1234
myCar.owner = Matt
myCar.make = Audi
…

How Applications Interact with the Ledger

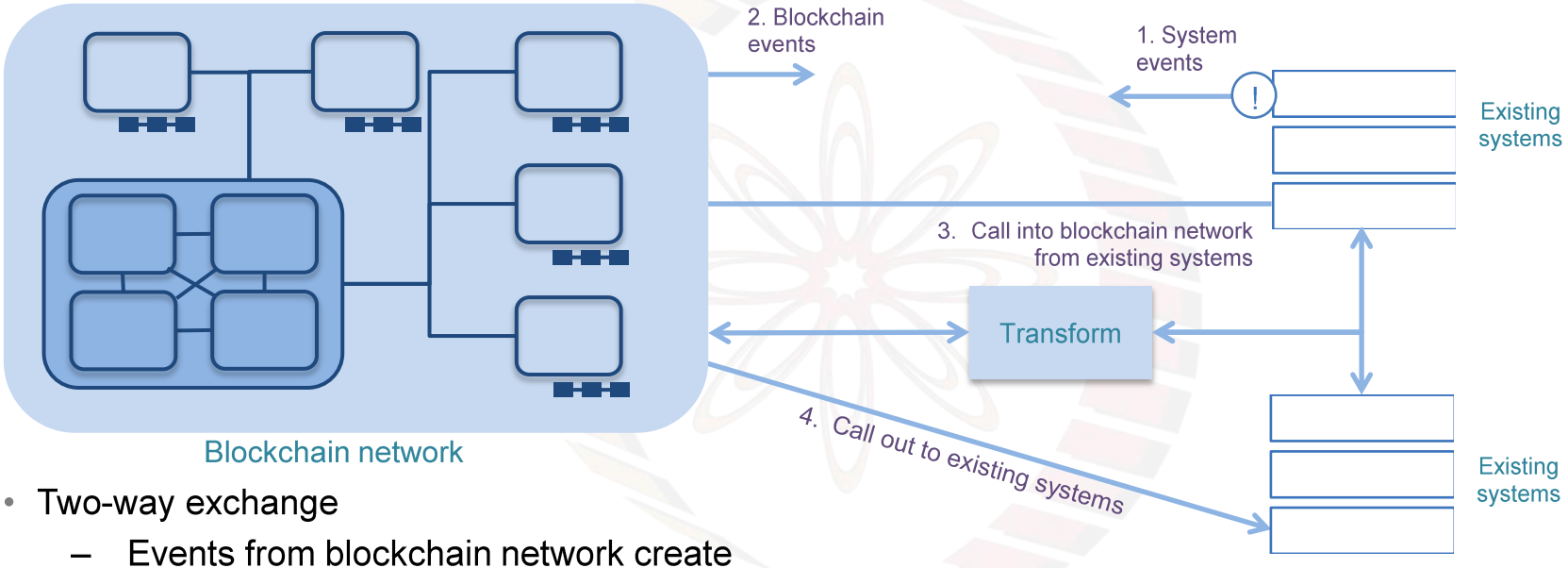


Blockchain Events

- In computing, an event is an occurrence that can trigger handlers
  - e.g. disk full, fail transfer completed, mouse clicked, message received, temperature too hot…
- Events are important in asynchronous processing systems like blockchain
- The blockchain can emit events that are useful to application programmers
  - e.g. Transaction has been validated or rejected, block has been added…
- Events from external systems might also trigger blockchain activity
  - e.g. exchange rate has gone below a threshold, the temperature has gone up, a time period has elapsed…



Integrating with Existing Systems – Possibilities



- Two-way exchange
  - Events from blockchain network create actions in existing systems
  - Cumulative actions in existing systems result in blockchain interaction
- Transformation between blockchain and existing systems' formats

Fun Reading

- Integrating Blockchain with ERP for a Transparent Supply Chain, Infosys white paper: *https://www.infosys.com/Oracle/white-papers/.../integrating-blockchain-erp.pdf*

- Introductory video to Hyperledger Fabric (3 mins): https://www.youtube.com/watch?v=JuXH9OYXcQQ
- Hyperledger Fabric Explainer (3 mins): https://www.youtube.com/watch?v=js3Zjxbo8TM

thank you!