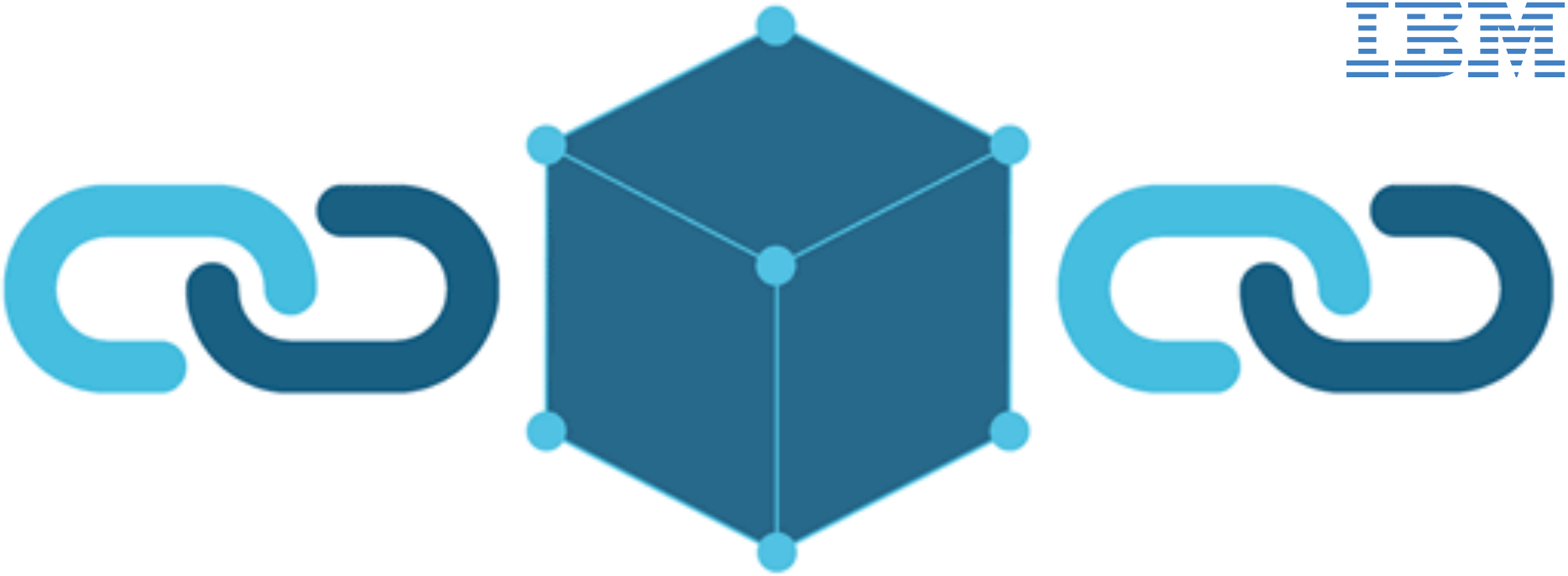


Blockchain Applications: Challenges, Opportunities, and Hyperledger Fabric

Bapi Chatterjee
bapchatt@in.ibm.com
IBM Research Lab
New Delhi, India

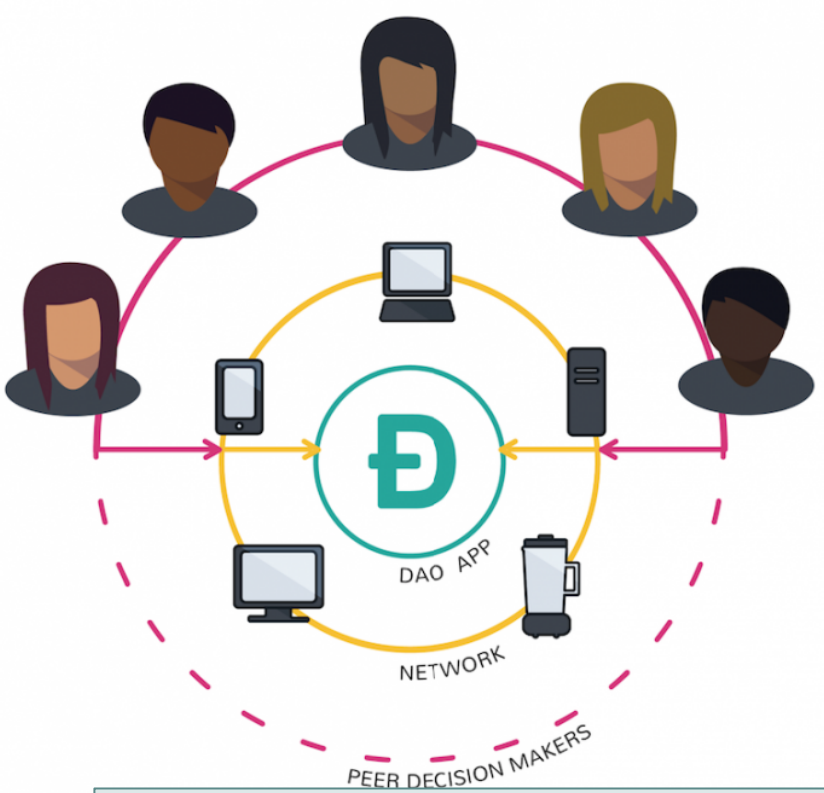
Disclaimer

- The statements/views expressed in the presentation slides are those of the presenter and should not be attributed to IBM in any manner whatsoever.
- The definitions, facts, numbers, etc. are true to the best of the knowledge of the presenter at the time when they were retrieved from their respective original sources.
- The presentation contains contents from external sources that are available publicly and the presenter duly acknowledges them.

Blockchain applications: How much do you know?

- Written a Chaincode/Smart-contract?
  - Solidity?
  - Fabric-composer?
  - Go?
  - Java?
- Know what can be done on a Blockchain?
- Mined Cryptocurrency?
  - BTC?
  - Ethereum?
  - …?
- Own BTC/Ethereum/…?

The DAO



What if the rules needed to be changed that is acceptable to all the participants?

Imagine this:

- A driverless car cruises around in search of passengers.
- After dropping someone off, the car uses its profits for a trip to a charging station.
- Except for it's initial programming, the car doesn't need outside help to determine how to carry out its mission.

Source: https://www.coindesk.com/information/what-is-a-dao-ethereum/

The BitNation

Lantmäteriet on Blockchain

The Land Registry in the blockchain

A development project with Lantmäteriet (The Swedish Mapping, cadastre and land registration authority), Telia Company, ChromaWay and Kairos Future

Lantmäteriet on Blockchain

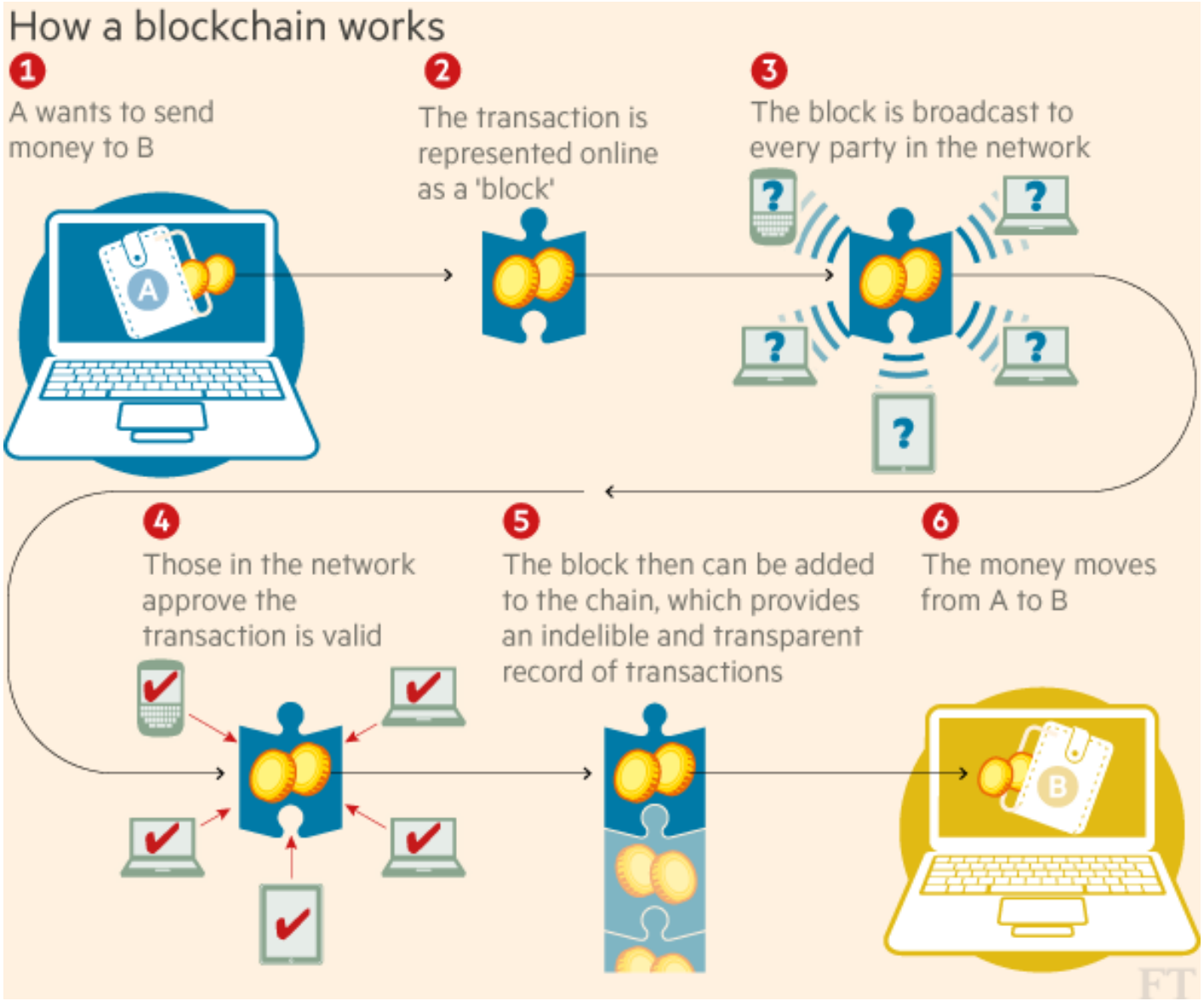
The Swedish system operates on a private blockchain. This has the land authority and others, like the banks, holding copies of the records. When a land title changes hands, each step of the process is verified and recorded on the blockchain (full details in this pdf). The system acts as a highly secure and transparent verification and storage service for property transactions, but it stops short of a full-blown cryptocurrency where land can be bought and sold as easily as a bitcoin. "There is no risk you will lose your land like you lose bitcoin," Kempe says.

The Land Registry in the blockchain

A development project with Lantmäteriet (The Swedish Mapping, cadastre and land registration authority), Telia Company, ChromaWay and Kairos Future

Source: https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/

How Blockchain Works



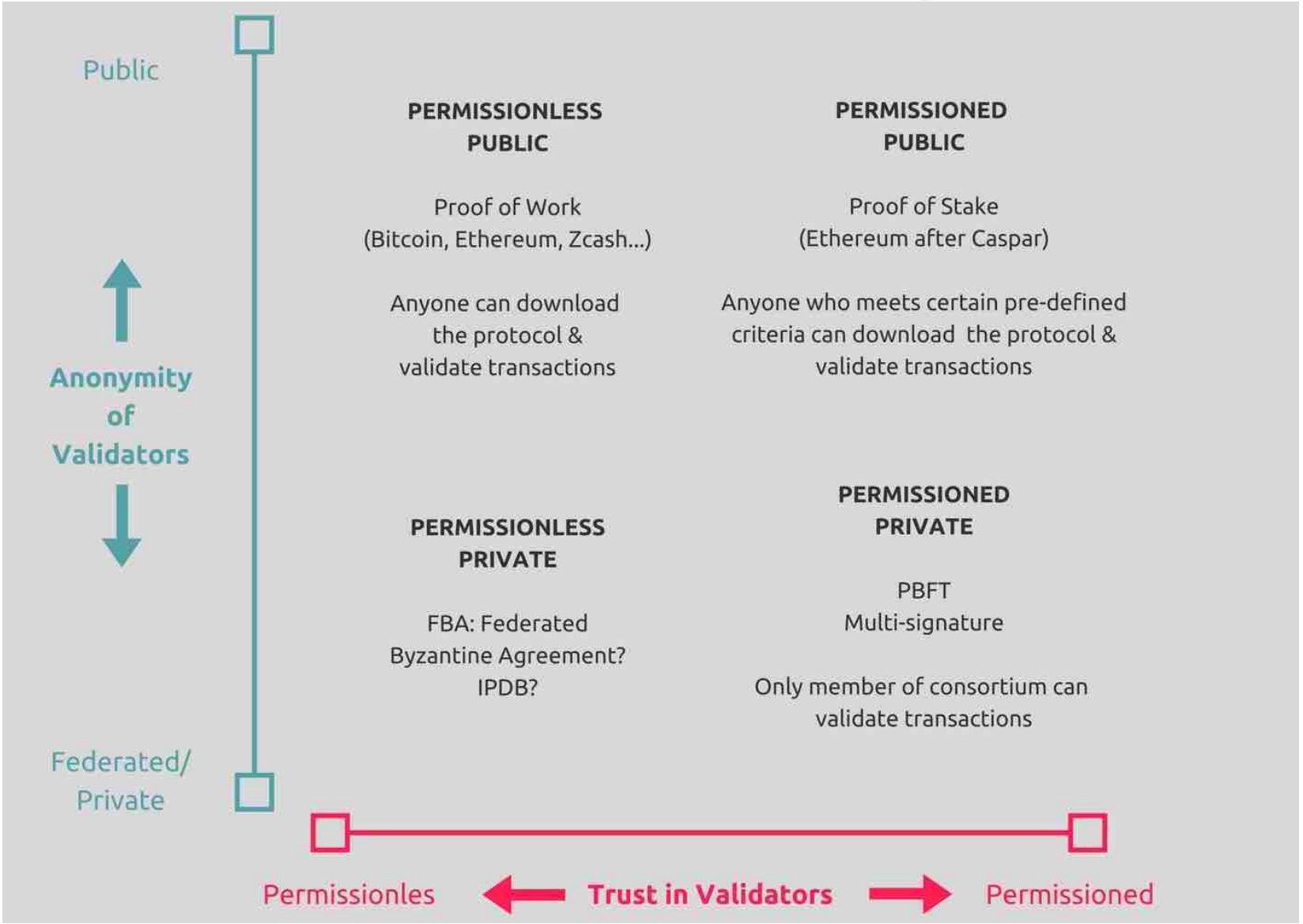
Source: https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/

The Blockchains

MultiChain

c·rda

The Blockchain Ecosystem



Source: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

The Blockchain Ecosystem

	Public No centralized management	Consortium Multiple Organizations	Private Single Organization
Participants	**Permissionless** •Anonymous •Could be malicious	**Permissioned** •Identified •Trusted	**Permissioned** - Identified - Trusted
Consensus Mechanisms	**Proof of Work, Proof of Stake, etc..** •Large energy consumption •No finality •51% attack	**Voting or multi-party consensus algorithm** •Lighter •Faster •Low energy consumption •Enable finality	**Voting or multi-party consensus algorithm** •Lighter •Faster •Low energy consumption •Enable finality
Transaction Approval Freq.	**Long** Bitcoin: 10 min or more	**Short** 100x msec	**Short** 100x msec
USP	**Disruptive** Disruptive in the sense of disintermediation. No middle men needed. Unclear what the business models will be	**Cost Cutting** Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency	**Cost Cutting** Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency

Source: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

The Blockchain Implementations

APPROACH	HOW IT IS DONE	EXAMPLES
IT Services	Build on request	ConsenSys
Blockchain First	Develop using the tools provided by the blockchain	Ethereum, Bitcoin
Development Platforms	Tools for IT Professionals	ERIS, Tendermint, Hyperledger
Vertical Solutions	Industry specific	Axoni, Chain, R3, itBit, Clearmatics
Special APIs & Overlays	DIY building blocks	Blockstack, Factom, Open Assets, Tierion

Source: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

A Simple Blockchain Implementation

Step 1: block structure.


```
1  class Block {
2      constructor(index, previousHash, timestamp, data, hash) {
3          this.index = index;
4          this.previousHash = previousHash.toString();
5          this.timestamp = timestamp;
6          this.data = data;
7          this.hash = hash.toString();
8      }
9  }
```


Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

Step 2: block hash.

```
1  var calculateHash = (index, previousHash, timestamp, data) => {
2      return CryptoJS.SHA256(index + previousHash + timestamp + data).toString();
3  };
```

Step 3: generate a block.

```
1  var generateNextBlock = (blockData) => {
2      var previousBlock = getLatestBlock();
3      var nextIndex = previousBlock.index + 1;
4      var nextTimestamp = new Date().getTime() / 1000;
5      var nextHash = calculateHash(nextIndex, previousBlock.hash, nextTimestamp, blockData);
6      return new Block(nextIndex, previousBlock.hash, nextTimestamp, blockData, nextHash);
7  };
```

Step 4: store a block.

```
1  var getGenesisBlock = () => {
2      return new Block(0, "0", 1465154705, "my genesis block!!", "816534932c2b7154836da6afc36
3  };
4
5  var blockchain = [getGenesisBlock()];
```


Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

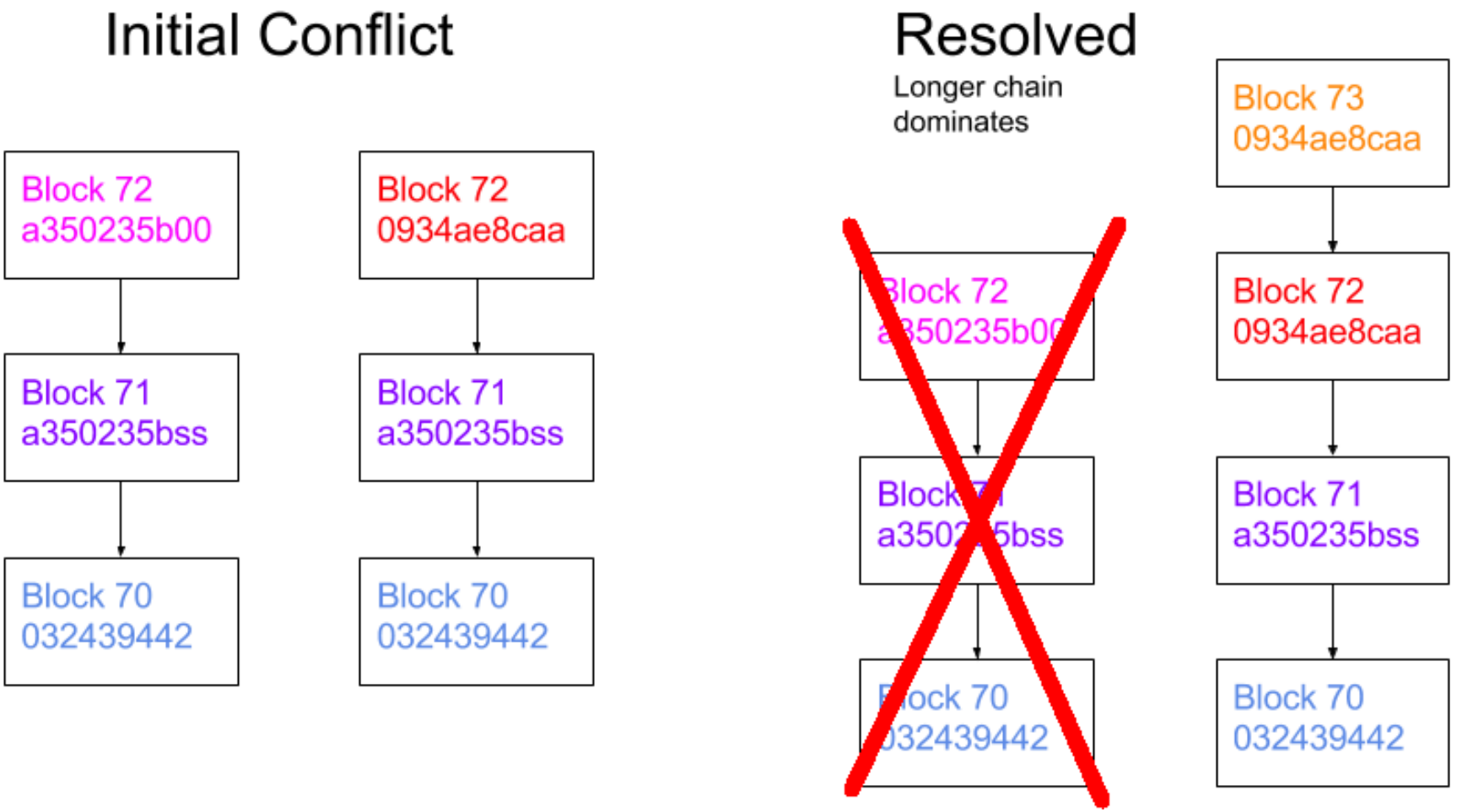
Step 5: check integrity of a block.

```
var isValidNewBlock = (newBlock, previousBlock) => {
    if (previousBlock.index + 1 !== newBlock.index) {
        console.log('invalid index');
        return false;
    } else if (previousBlock.hash !== newBlock.previousHash) {
        console.log('invalid previoushash');
        return false;
    } else if (calculateHashForBlock(newBlock) !== newBlock.hash) {
        console.log('invalid hash: ' + calculateHashForBlock(newBlock) + ' ' + newBlock.has
        return false;
    }
    return true;
};
```


Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

Step 6: choose the longest chain.



Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

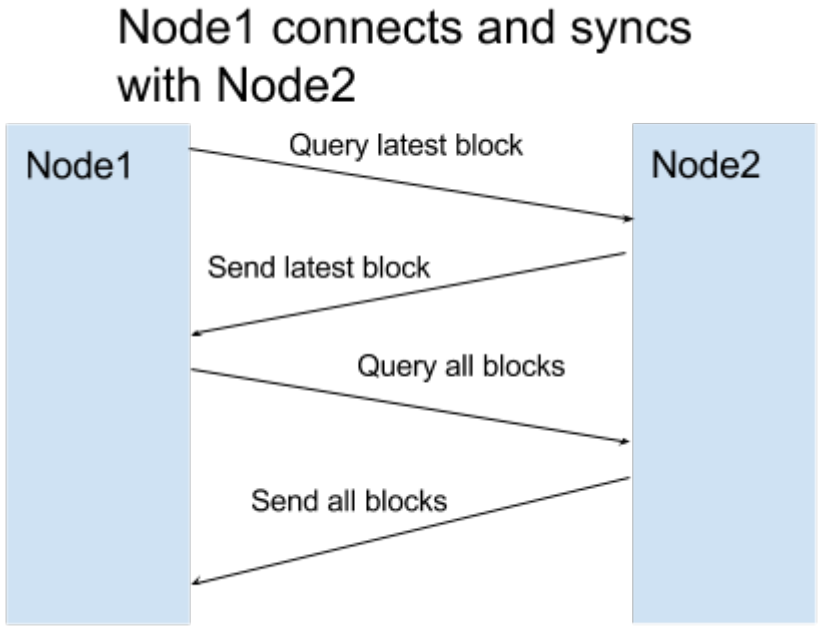
Step 6: choose the longest chain.

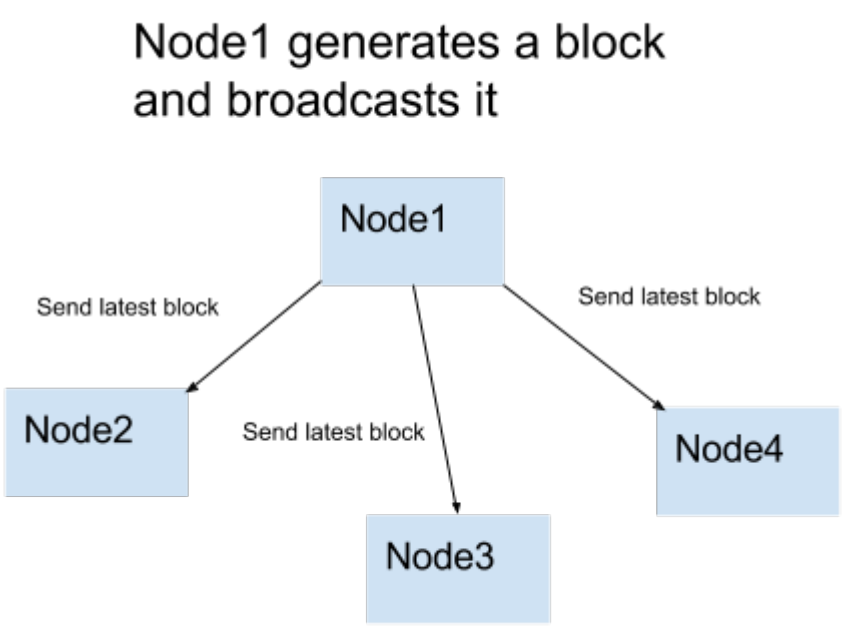
```
var replaceChain = (newBlocks) => {
    if (isValidChain(newBlocks) && newBlocks.length > blockchain.length) {
        console.log('Received blockchain is valid. Replacing current blockchain with receive
        blockchain = newBlocks;
        broadcast(responseLatestMsg());
    } else {
        console.log('Received blockchain invalid');
    }
};
```


Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

Step 7: communicate with other nodes.





Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

A Simple Blockchain Implementation

Step 7: control the nodes.

```
1  var initHttpServer = () => {
2      var app = express();
3      app.use(bodyParser.json());
4
5      app.get('/blocks', (req, res) => res.send(JSON.stringify(blockchain)));
6      app.post('/mineBlock', (req, res) => {
7          var newBlock = generateNextBlock(req.body.data);
8          addBlock(newBlock);
9          broadcast(responseLatestMsg());
10         console.log('block added: ' + JSON.stringify(newBlock));
11         res.send();
12     });
13     app.get('/peers', (req, res) => {
14         res.send(sockets.map(s => s._socket.remoteAddress + ':' + s._socket.remotePort));
15     });
16     app.post('/addPeer', (req, res) => {
17         connectToPeers([req.body.peer]);
18         res.send();
19     });
20     app.listen(http_port, () => console.log('Listening http on port: ' + http_port));
21 };
```


Source: https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

Hyperledger Fabric

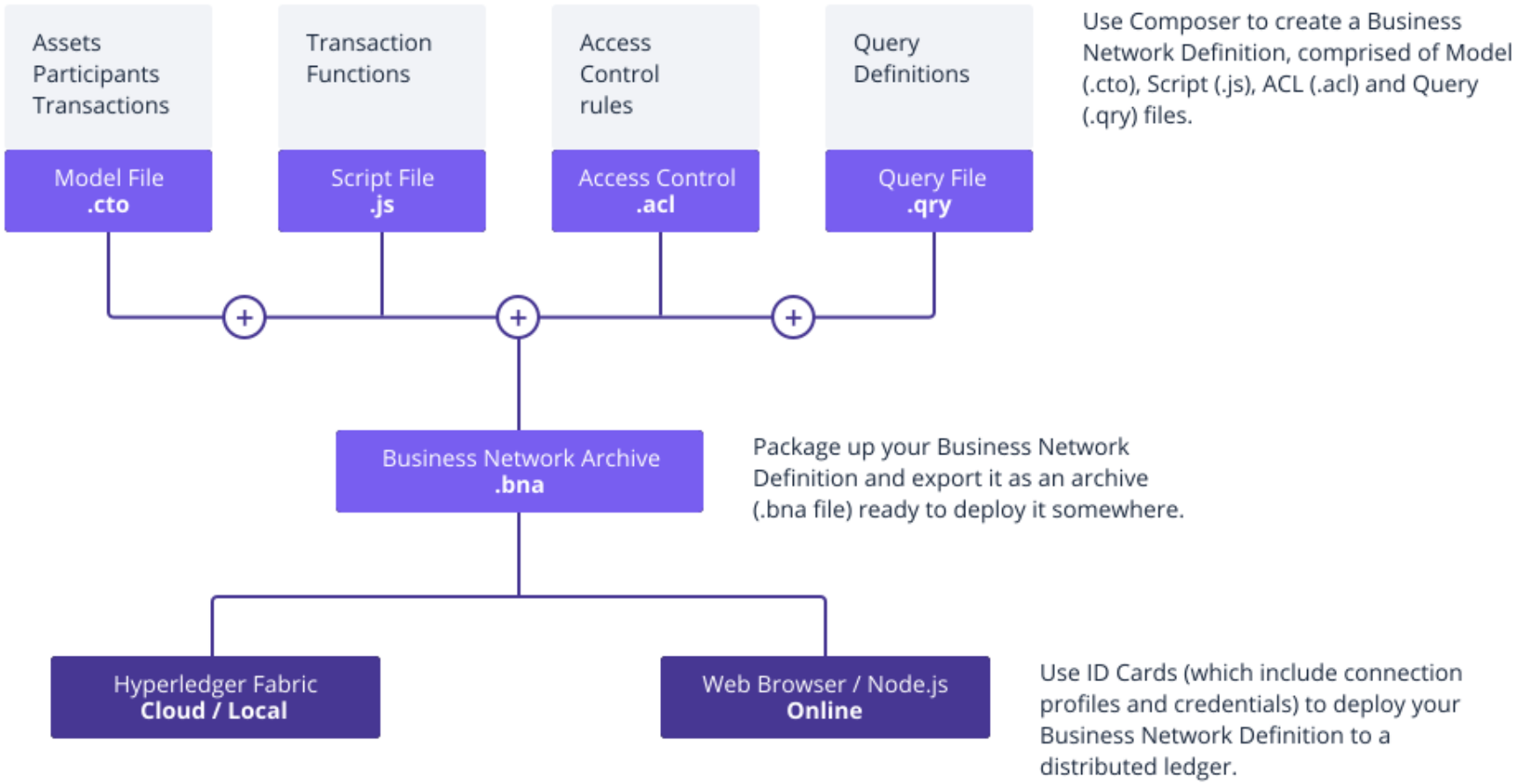
HYPERLEDGER

Hyperledger Fabric SDK

HYPERLEDGER

FABRIC SDK Go

Hyperledger Fabric Composer



https://www.ibm.com/developerworks/cloud/library/cl-model-test-your-blockchain-network-with-hyperledger-composer-playground/index.html

Blockchain will disrupt every industry!

Thanks!

You know how it works.