

Blockchain For Business On Hyperledger

Anna Derbakova
Software Engineer (IBM Blockchain)

HYPERLEDGER



What is blockchain?



Bitcoin



=

Two Innovations

An Economic Innovation



A topic for another day...

A Technological Innovation

How is it possible that strangers on the internet can agree on the accounting of over **\$5,000,000,000** with no central authority?

A Technological Innovation

How is it possible that strangers on the internet can agree on the accounting of over **\$5,000,000,000** with no central authority?

Answer: Blockchain

More Than Bitcoin...

THE WALL STREET JOURNAL. [Subscribe Now](#)


[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) **[Business](#)** [Tech](#) [Markets](#) [Opinion](#) [Arts](#) [Life](#) [Real Estate](#)

Wal-Mart Turns To Blockchain For Tracking Pork In China

The retailer aims to better verify parties that handle the meat as it winds through complex supply chains

By KIM S. NASH
Oct 19, 2016 4:43 pm ET

0 COMMENTS



A vendor selling pork at a market in Qingdao, east China's Shandong Province, October 14th. Wal-Mart Stores Inc. plans to use blockchain technology to improve food safety in China. PHOTO: SIPA ASIA VIA ZUMA PRESS

CONTENT FROM OUR SPONSOR

Deloitte.

CIO Insights and Analysis from Deloitte

Social Impact of Exponential Technologies

Harnessing exponential technologies for social impact can allow organizations to address pressing societal issues, build new markets, and attract top talent and consumers. CIOs can help drive their companies' exponential initiatives for both philanthropic good and for more commercial purposes as well.

Please note: The Wall Street Journal News Department was not involved in the creation of the content above.

[More from Deloitte](#)

Most Popular Videos

Gay Couple Gets

“Consumers today want more transparency about where and how a product came to be.”

Frank Yiannas, vice president of food safety at Walmart

<http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/>

<http://blogs.wsj.com/cio/2016/10/19/wal-mart-turns-to-blockchain-for-tracking-pork-in-china/>

<http://www.forbes.com/sites/yanzhonghuang/2014/07/16/the-2008-milk-scandal-revisited/#5adf77064428>

Blockchain

- Database
- Consensus Algorithms
- Peer-to-peer Communication
- Cryptography

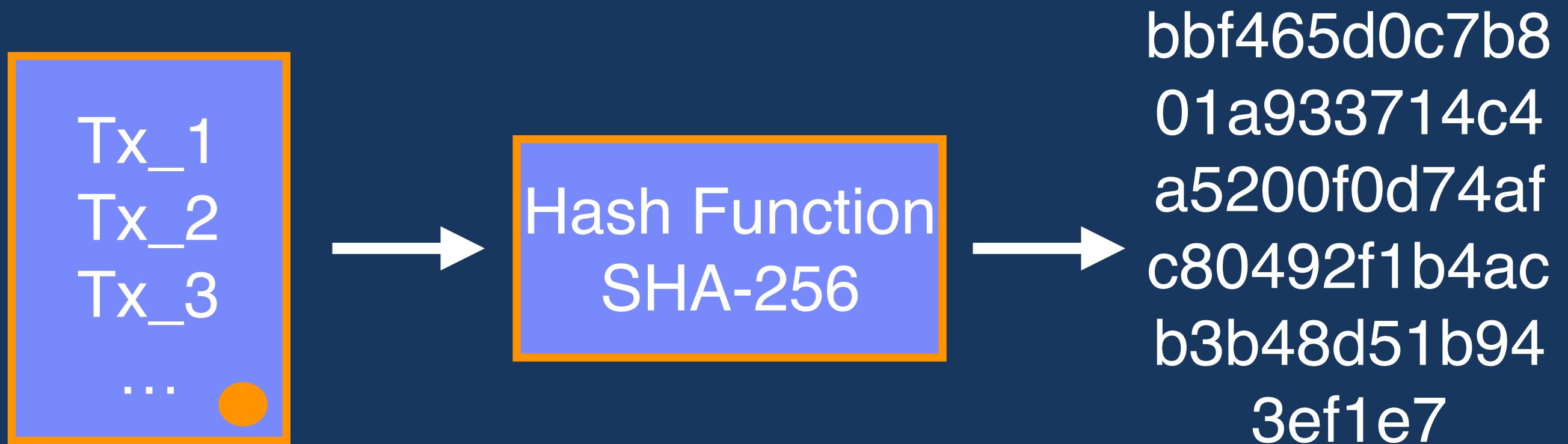
Block—chain

- Hash — Fingerprint of data



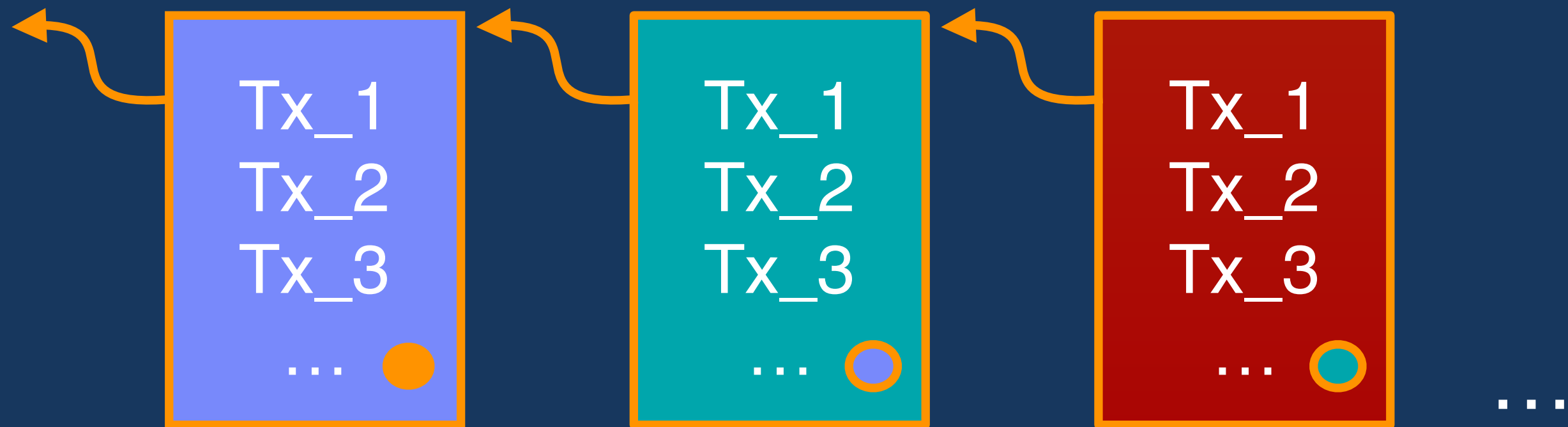
Block—chain

- Block — Collection of transactions + hash of previous block



Block—chain

- Block — Collection of transactions + hash of previous block



Block—chain

- Block — Collection of transactions + hash of previous block



Blockchain

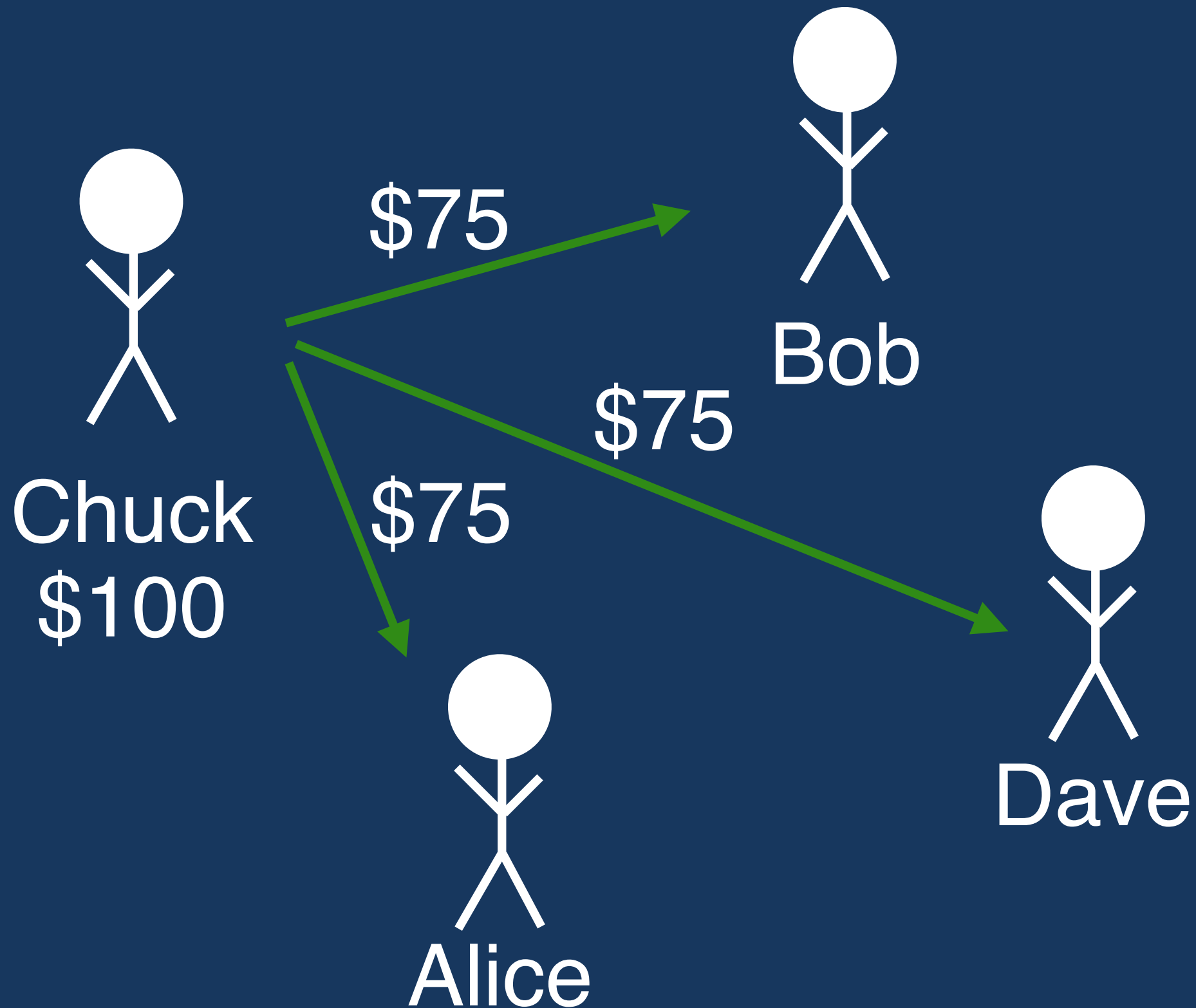
- Database
- Consensus Algorithms
- Peer-to-peer Communication
- Cryptography

The Really Hard Stuff

Consensus



Consensus



Which check
will bounce?

Blockchain

- Database
- Consensus Algorithms
- Peer-to-peer Communication
- Cryptography

Business Use Cases

Asset Transfer

- Anything that is capable of being owned or controlled to produce value, is an asset
- Two fundamental types of assets
 - Tangible, e.g. a house
 - Intangible e.g. a mortgage
- Intangible assets subdivide
 - Financial, e.g. bond
 - Intellectual e.g. patents
 - Digital e.g. music
- Cash is also an asset



Transferring An Asset

- Asset is codified within a (smart) contract
- Asset is exchanged by updating contract state through an available action

vehicleState:

```
var vin  
var manufacturer  
var make  
var model  
var year  
var owner
```

vehicleContract:

```
createVehicle  
scrapVehicle  
updateOwner
```

Pork Supply Chain



Hyperledger Project

Hyperledger Project

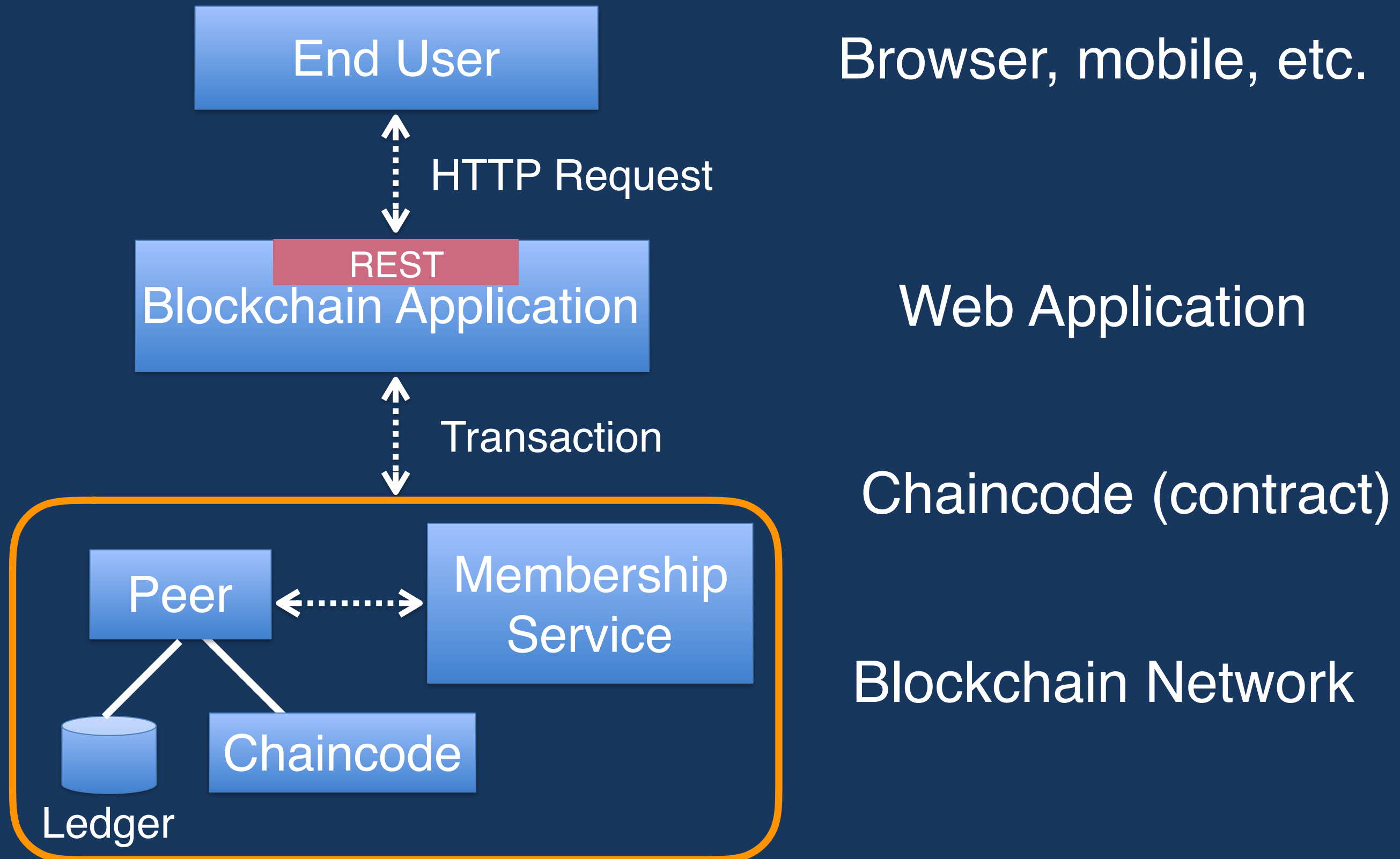
- Cross-industry collaborative effort to support blockchain-based distributed ledgers
- Focused on ledgers designed to support global business transactions
- Develop open protocols and standards for supporting blockchain
- <https://www.hyperledger.org/>

How Is Hyperledger Different?

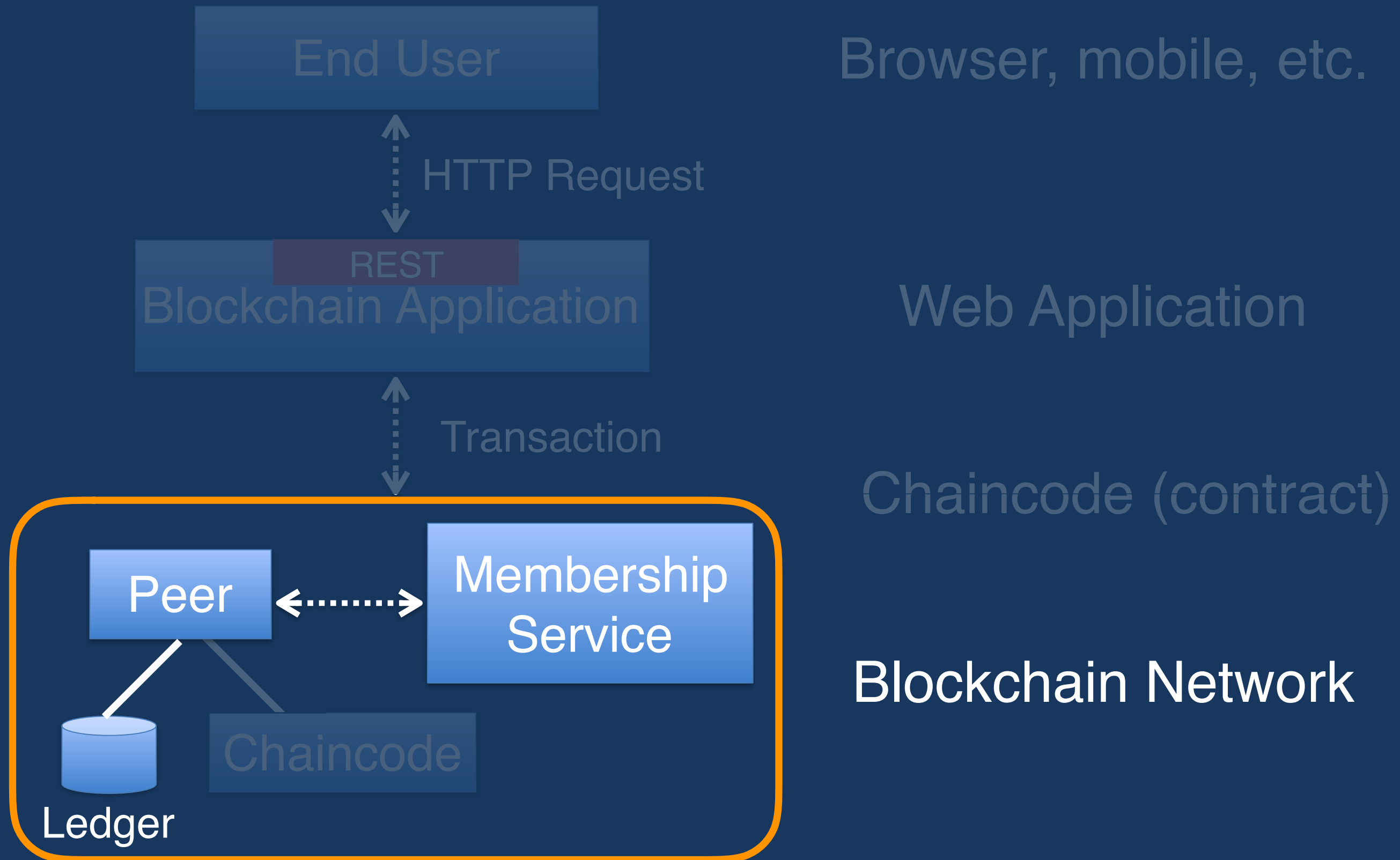
- Permissioned blockchain
- No miners or coins
- Provides a modular framework that supports different components for different uses
- Other consensus schemes, like PBFT (Practical Byzantine Fault Tolerance) may be used

Let's Build an app!

Blockchain Application

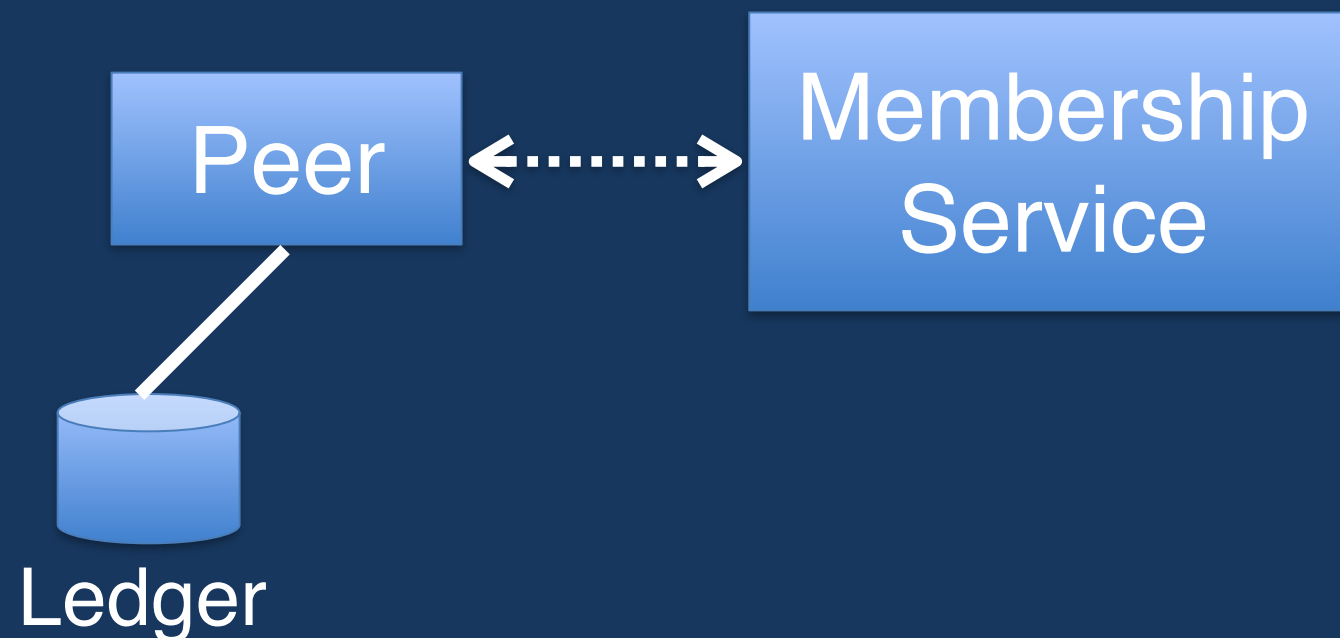


Blockchain Network



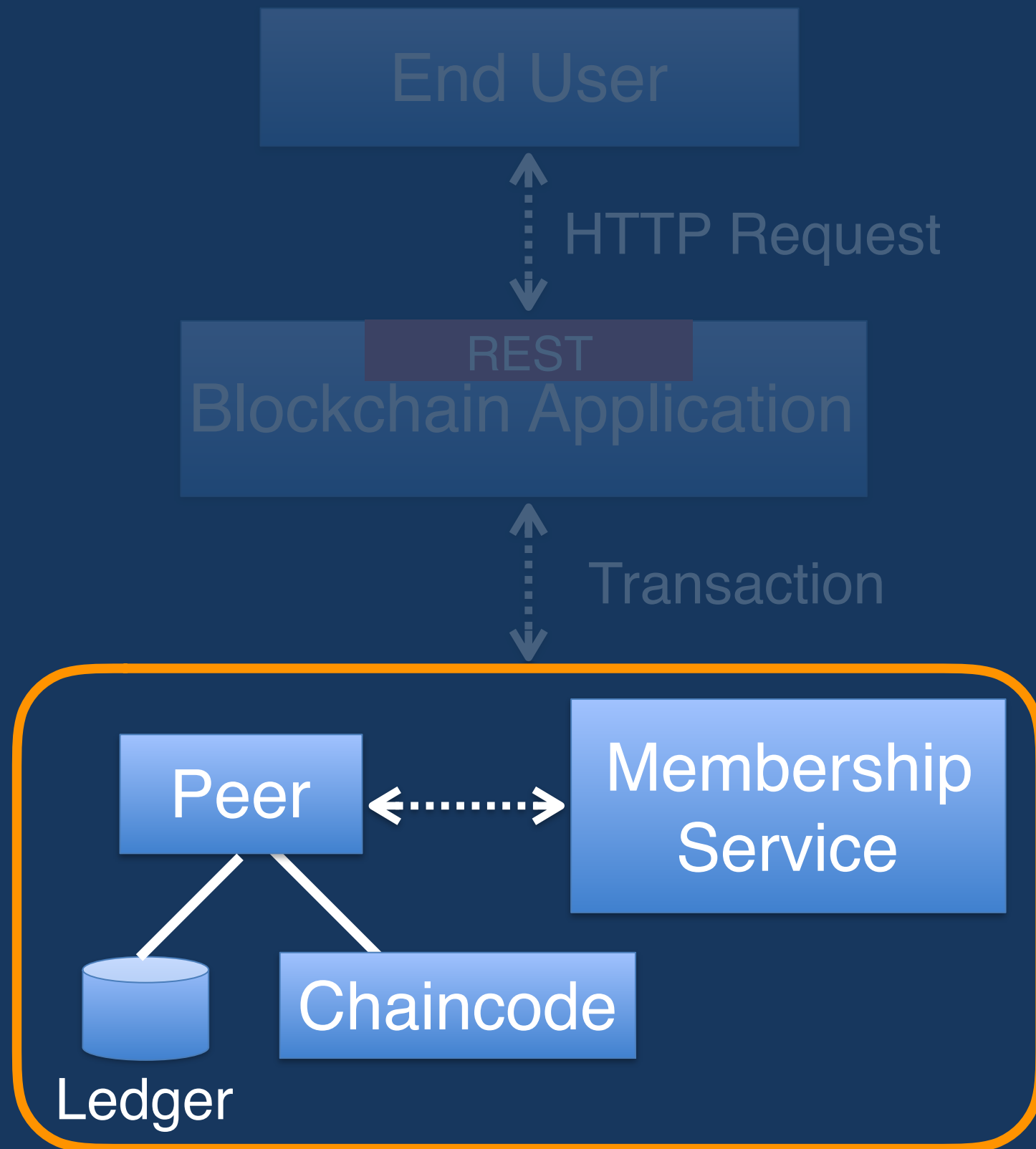
Blockchain Network

- Docker images provided
- Single peer + membership service
- Four peers + membership service



docker

Chaincode (Smart Contract)



Browser, mobile, etc.

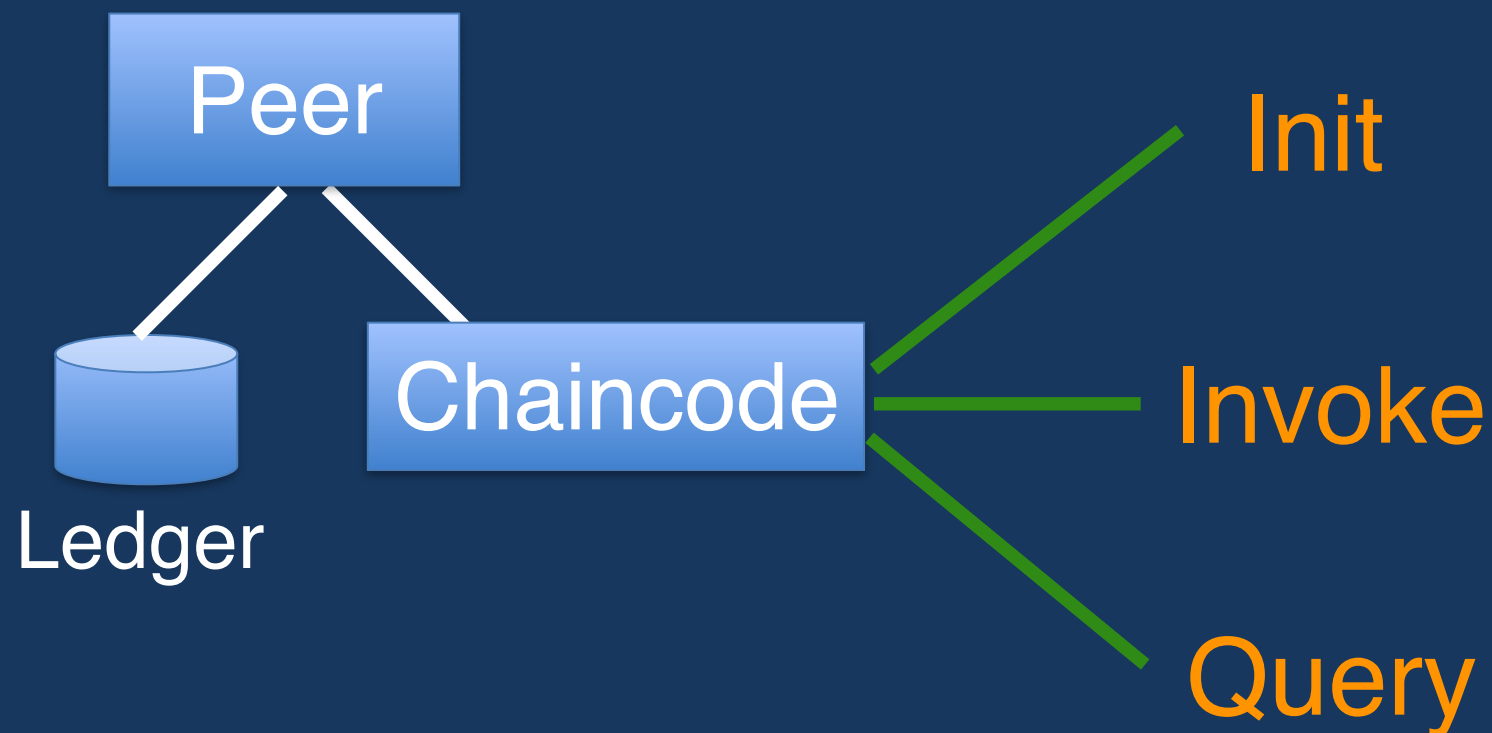
Web Application

Chaincode (contract)

Blockchain Network

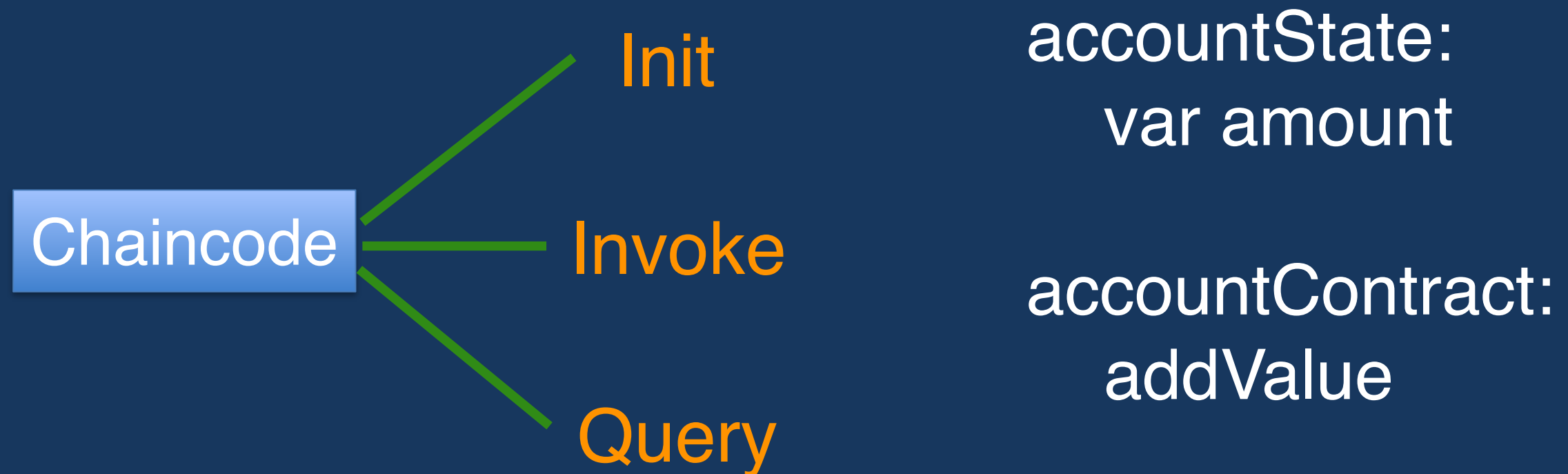
Chaincode (Smart Contract)

- Implemented in Go
- Packaged together with dependencies
- Docker container running on the validating peer



Crowd Funding Chaincode

- Stores the “account” state variable
- Invoke action adds value to “account”
- Query action retrieves the value of “account”



Web Application

End User

Browser, mobile, etc.

HTTP Request

REST

Blockchain Application

Web Application

Transaction

Chaincode (contract)

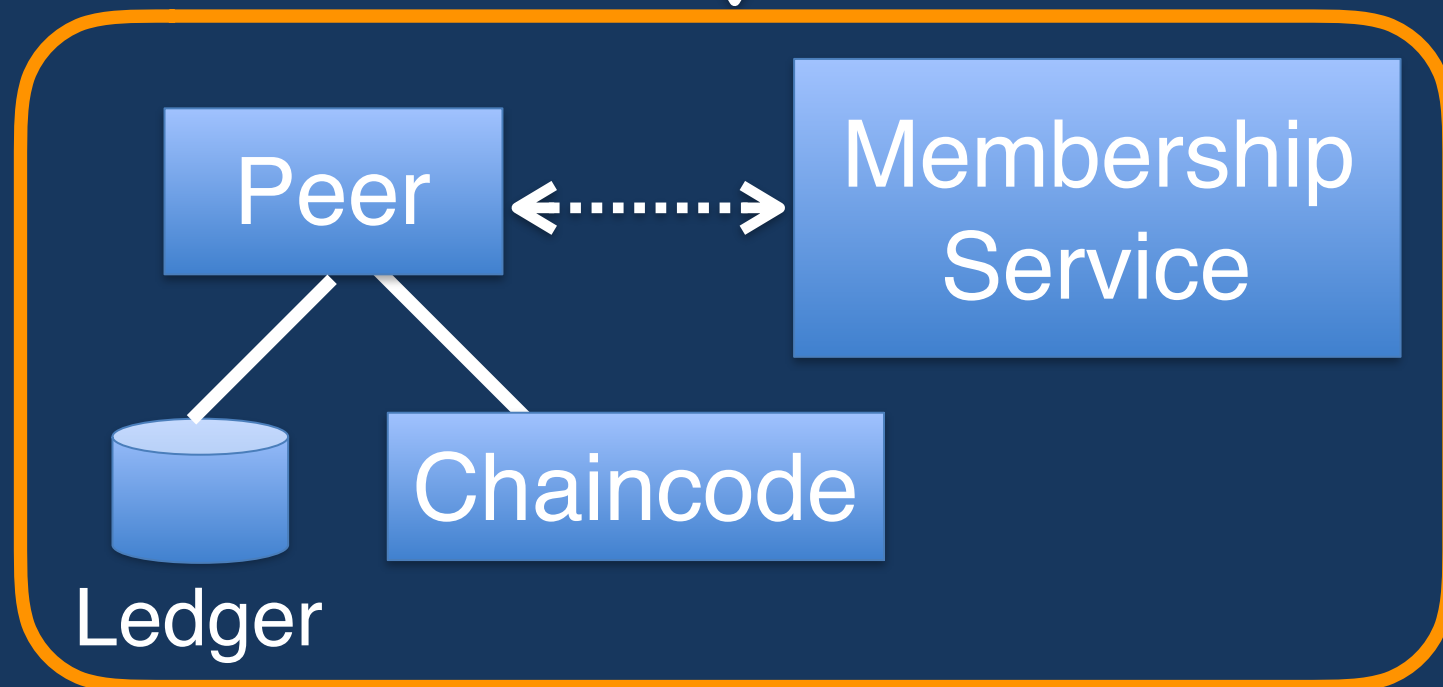
Peer

Membership
Service

Blockchain Network

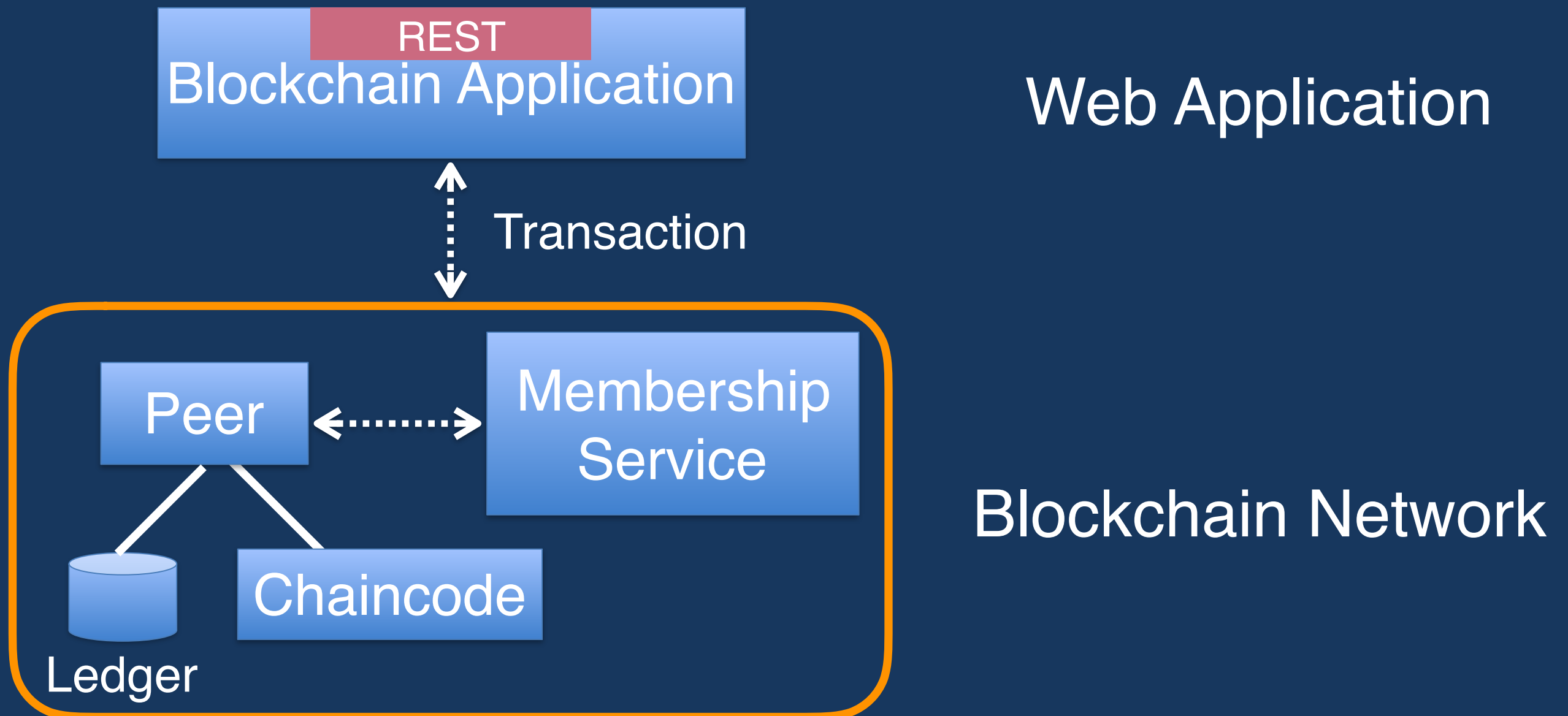
Chaincode

Ledger



Web Application

- Implemented with Node.js (uses the “hfc” NPM module)
- Registers and enrolls users
- Deploys, invokes, and queries the chaincode



Front End Application

End User

Browser, mobile, etc.



HTTP Request

REST

Blockchain Application

Questions?

Getting Started Tutorial: <http://bit.ly/hyperledger-basics>

Anna Derbakova: adderbak@us.ibm.com
<https://www.linkedin.com/in/annadderbakova>

Backup

Proof of Work*



Alice

\$100

Honest



Bob

\$100

Honest



Chuck

\$100

Dishonest



Dave

\$100

Honest

Our Simple Bank has four account holders and no central authority. How can we reach consensus on our account values?

*This simplistic example leaves out details for the purpose of explaining PoW in 5 minutes.

Proof of Work



Alice

\$100

Honest



Bob

\$100

Honest



Chuck

\$100

Dishonest



Dave

\$100

Honest

Everyone starts trying to solve a very difficult (but easily verifiable) problem. It's so difficult, with four people working, it will only be solved once every 10 minutes.

Proof of Work



Alice

\$100

Honest



Bob

\$100

Honest



Chuck

\$100

Dishonest



Dave

\$100

Honest

While attempting to solve the problem, our actors also announce transactions.

Alice - send \$50 to Dave

Bob - send \$20 to Alice

Chuck - send \$1,000 to Dave

Proof of Work



Alice

\$100



Bob

\$100



Chuck

\$100



Dave

\$100

Alice solves the problem first. She announces the solution.

Alice's
block

Valid transactions Alice heard
= hash(solution + Alice - send \$50 to Dave
Bob - send \$20 to Alice)

Proof of Work



Alice

\$70

Honest



Bob

\$80

Honest



Chuck

\$100

Dishonest



Dave

\$150

Honest

After verifying Alice's solution, everyone starts working on a new problem that includes the hash of Alice's block.

Alice's
block

Proof of Work



Alice

\$70

Honest



Bob

\$80

Honest



Chuck

\$100

Dishonest



Dave

\$150

Honest

Bob finds
the next
solution.

Alice's
block



Bob's
block

= hash (solution +

New transactions

Dave - send \$10 to Bob)

Dave - send \$20 to Alice

Proof of Work



Alice

\$90

Honest



Bob

\$90

Honest



Chuck

\$100

Dishonest



Dave

\$120

Honest

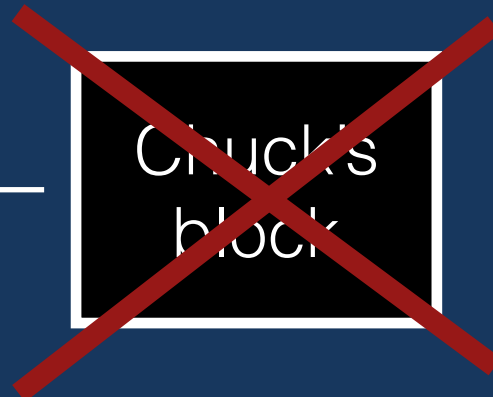
Chuck finds the next solution, but includes fake transactions his block.

Alice, Bob, and Dave ignore his block and keep looking for another solution.

Alice's
block

Bob's
block

Chuck's
block



Proof of Work



Alice

\$90

Honest



Bob

\$90

Honest



Chuck

\$100

Dishonest



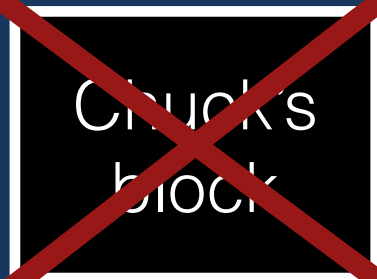
Dave

\$120

Honest

Chuck finds the solution again, but he doesn't include previous blocks in an attempt to erase old transactions.

Again, he is ignored because it's not the longest chain.



Proof of Work



Alice

\$90

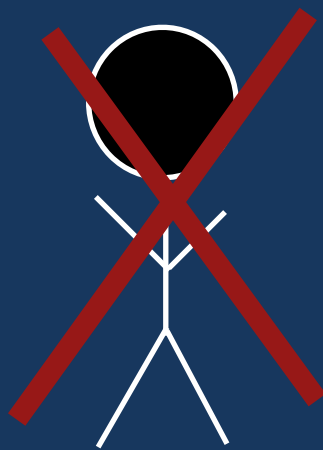
Honest



Bob

\$90

Honest



Chuck

\$100

Dishonest



Dave

\$120

Honest

Chuck can't
fake a longer
chain because
solving these
problems
requires too
much work.
Chuck gives
up!

Alice's
block



Bob's
block