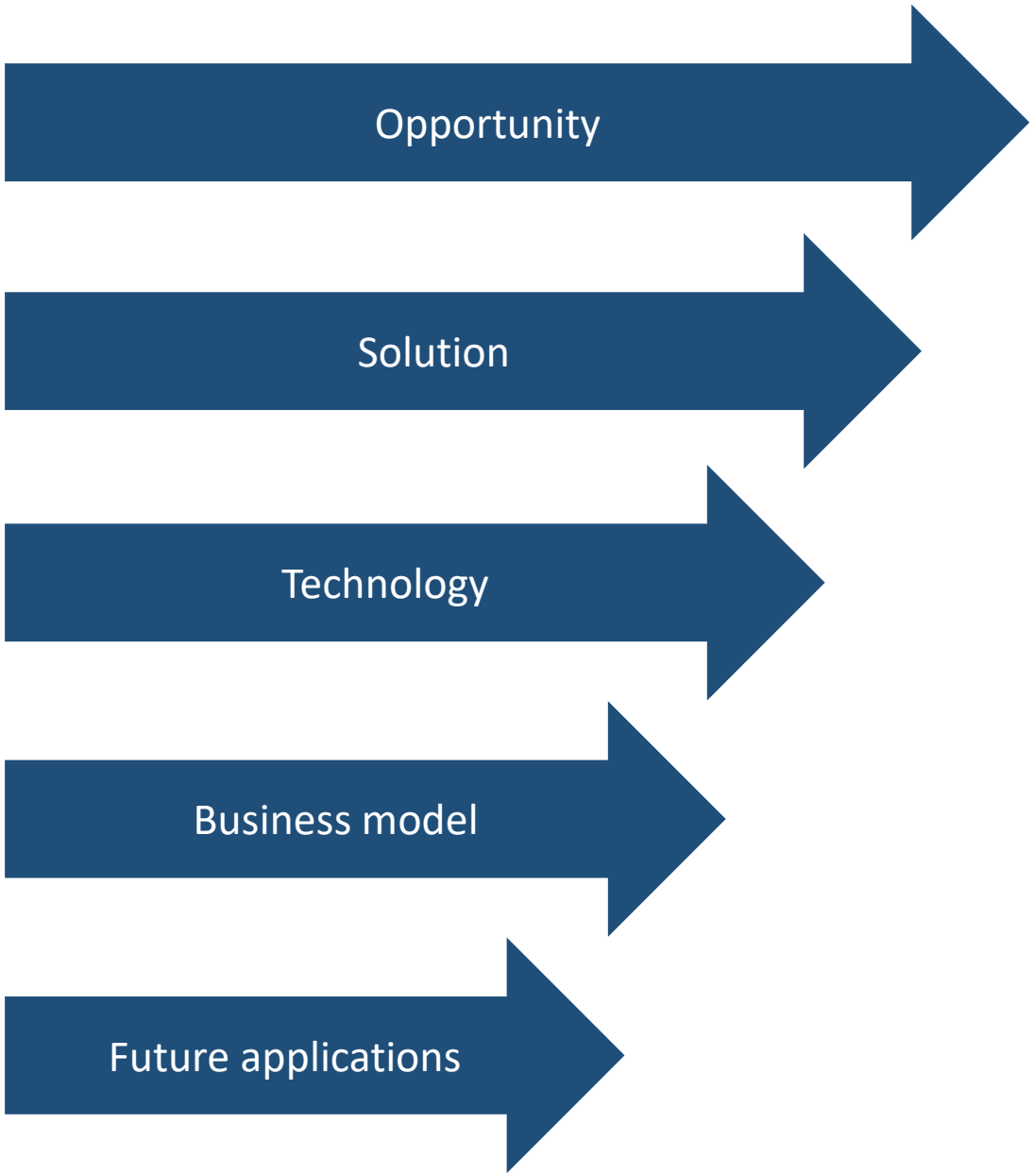
Bitcoin and Cryptocurrencies

- Lecture 7: Identity
- Professor Radjabov Mukhammad

Executive Summary



Current IoT solutions rely on a centralized model that creates inefficient and unsecured environment with high costs and limited connection between devices.

Smart digital identity using Blockchain technology. The identity will reduce costs, improve security, and increase interconnectivity.

Use DigID profile to log into IoT devices, after which usage information and preferences will be stored and shared on the blockchain.

Freemium model. Subscription based charges for more than 10 devices. Direct sales combined with white-label partnership.

The convergence of Blockchain identity and IoT creates endless possibilities for applications in many industries such as consumer electronics, automotive and shipping.

Problem/Opportunity

How ready are we for the smart home?

FORTUNE | 5 reasons why the 'smart home' is still stupid

ONE HUB/ONE DASHBOARD/ONE ANYTHING

: To achieve the *Her*-like experience or even a great artificial intelligence, you need a central place for all of your smart home information. Maybe it's a hub, maybe it's a router, maybe it's software on your phone or in the cloud, but everything in your home has to talk to this central hub. It should also should have some kind of mechanism to tell the consumer why their bedroom lights turn on at 7 am. Right now, most companies are fighting to provide this software, which is causing no end of drama for the consumer and other players trying to build a business in the smart home. For example, Apple just started certifying gadgets under its HomeKit program, but not every gadget will work with the program, and Android users won't be able to use it at all. Meanwhile, many physical hubs only work with certain devices, leading consumers to be confused about what works with what.

BuzzFeedNEWS

Survey Says: People Have Way Too Many Passwords To Remember

According to the online survey, which surveyed more than 2,000 English-speaking adults, the average person has 27 discrete online logins.

"The sheer number of accounts has grown dramatically over the past few years," said Bruce Snell, Cybersecurity and Privacy Director at Intel Security.

While a cluster of password managers like Dashlane, 1Password and Passpack have emerged to help address the issue, most people don't use one. Which perhaps explains why, according to the study, 37% percent of people forget a password at least once a week.

Last Friday saw **a massive internet outage** after hackers flooded **Dyn**, a major internet gatekeeper for sites like Facebook, Spotify and Netflix, with false bandwidth from an ocean of unsecured internet-connected devices.

Many of these devices were **reportedly smart home gadgets using standardized manufacturer default passwords**. It's alarmingly easy for hackers to search the web for these devices and then, with the right malware, take control of them en masse. From there, the hackers can use their army of hacked devices, called a "botnet," to **overwhelm whatever server they aim it at**.

The episode raises some serious questions about the **smart home**. More and more people are filling their living spaces with an ever-increasing number of internet-connected devices. That means more potential fodder for the next big botnet, and fears of even bigger attacks in the future.

The problem with the centralized model

Current IoT ecosystems rely on centralized, brokered communication models, otherwise known as the server/client paradigm. All devices are identified, authenticated and connected through cloud servers that sport huge processing and storage capacities. Connection between devices will have to exclusively go through the internet, even if they happen to be a few feet apart.

While this model has connected generic computing devices for decades, and will continue to support small-scale IoT networks as we see them today, it will not be able to respond to the growing needs of the huge IoT ecosystems of tomorrow.

Existing IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized clouds, large server farms and networking equipment. The sheer amount of communications that will have to be handled when IoT devices grow to the tens of billions will increase those costs substantially.

Problem/Opportunity

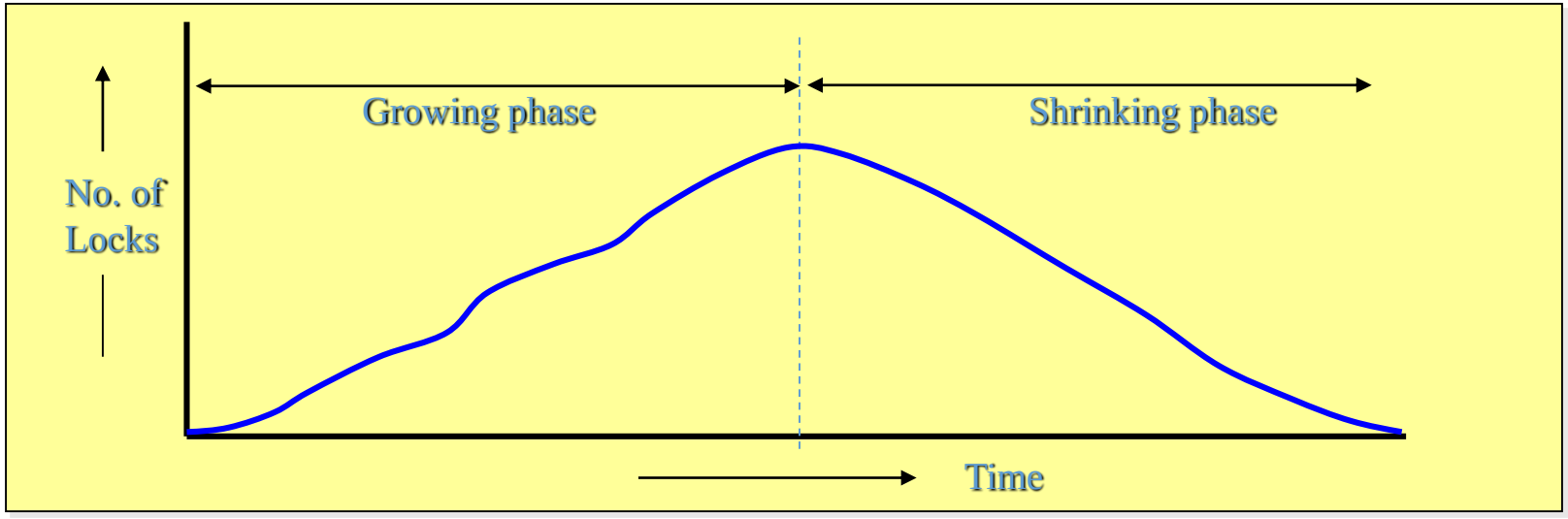
SMART HOME DEVICES FACE BOTTLENECK

1. High infrastructure and maintenance costs associated with the current centralized model
2. Connection between smart home devices is limited
3. There is no single platform that connects all devices
4. Too many online accounts and passwords
5. Our information online is susceptible to hacking

Proposed solution : Smart digital identity

Two Phase Locking (2PL) Protocols

- In 2PL—All *lock* operations must precede the first *unlock* operation
  - Two phases
    - expanding or growing phase: all locking are done in this phase but no lock release allowed

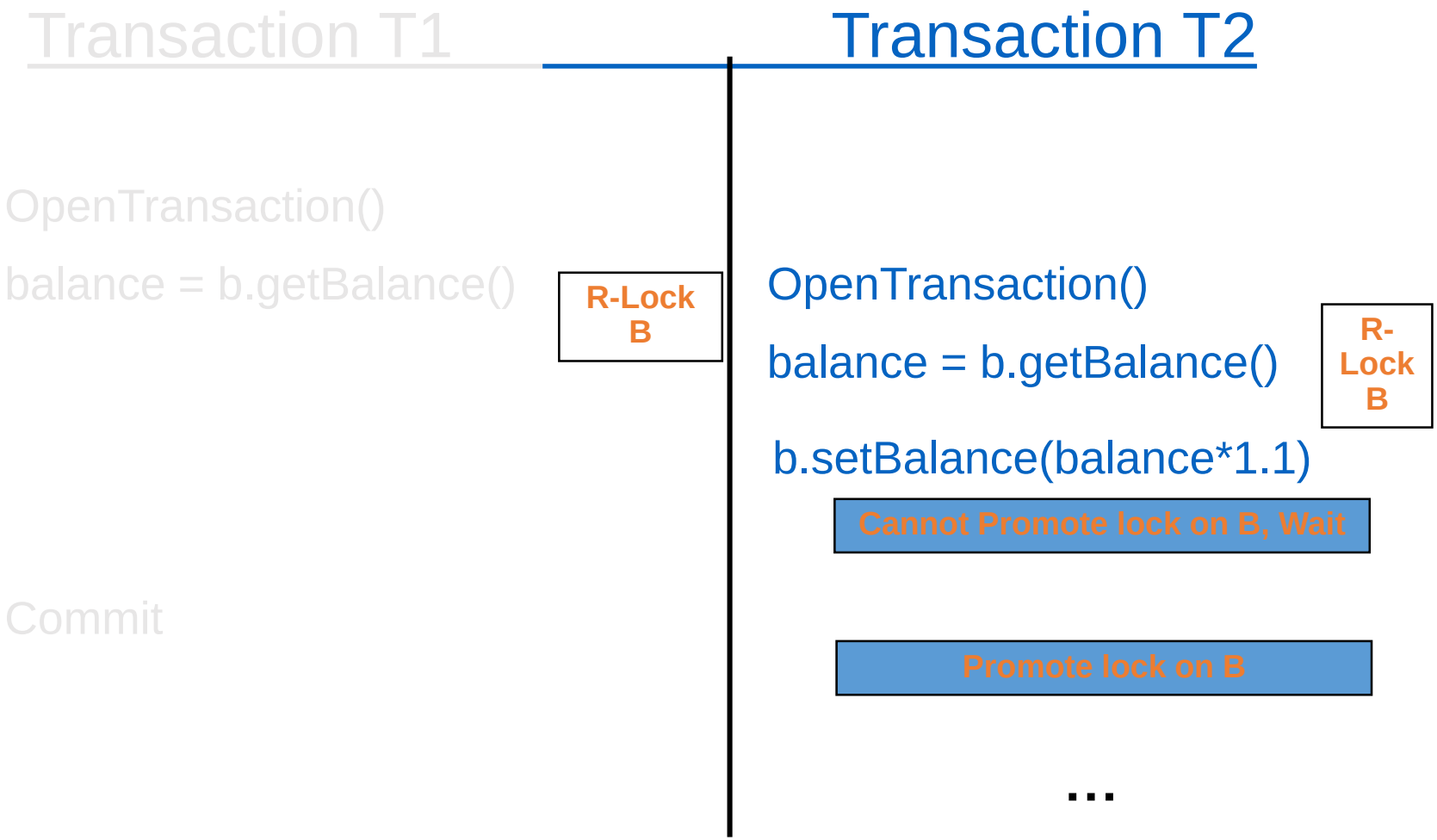


Locking Procedure in Strict-2P Locking

- When an operation accesses an object:
  - if you can, promote a lock (nothing -> read -> write)
  - Don't promote the lock if it would result in a conflict with another transaction's already-existing lock
    - wait until all shared locks are released, then lock & proceed
- When a transaction commits or aborts:
  - release all locks that were set by the transaction

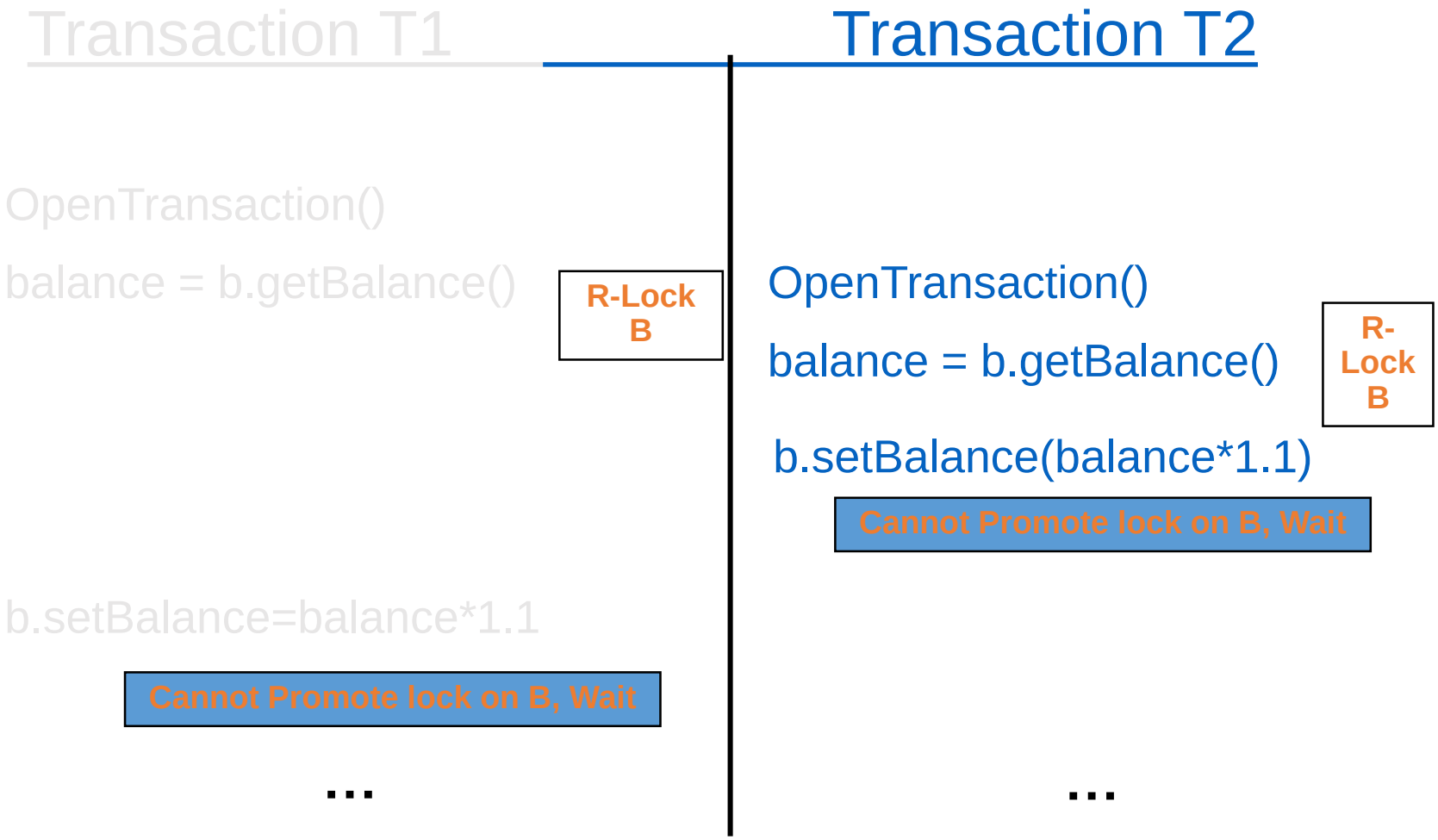
Example: Concurrent Transactions

- Non-exclusive Locks



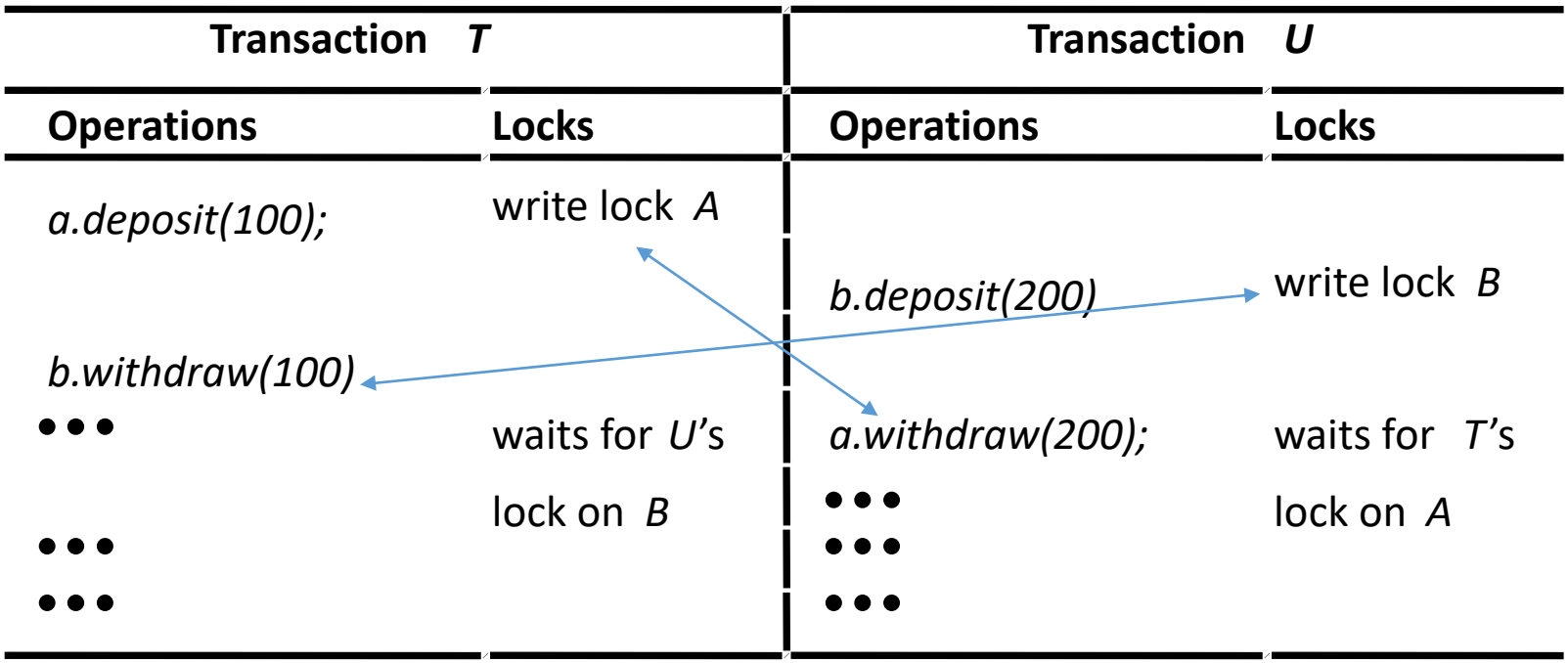
Example: Concurrent Transactions

- What happens in the example below?



Deadlock with write locks

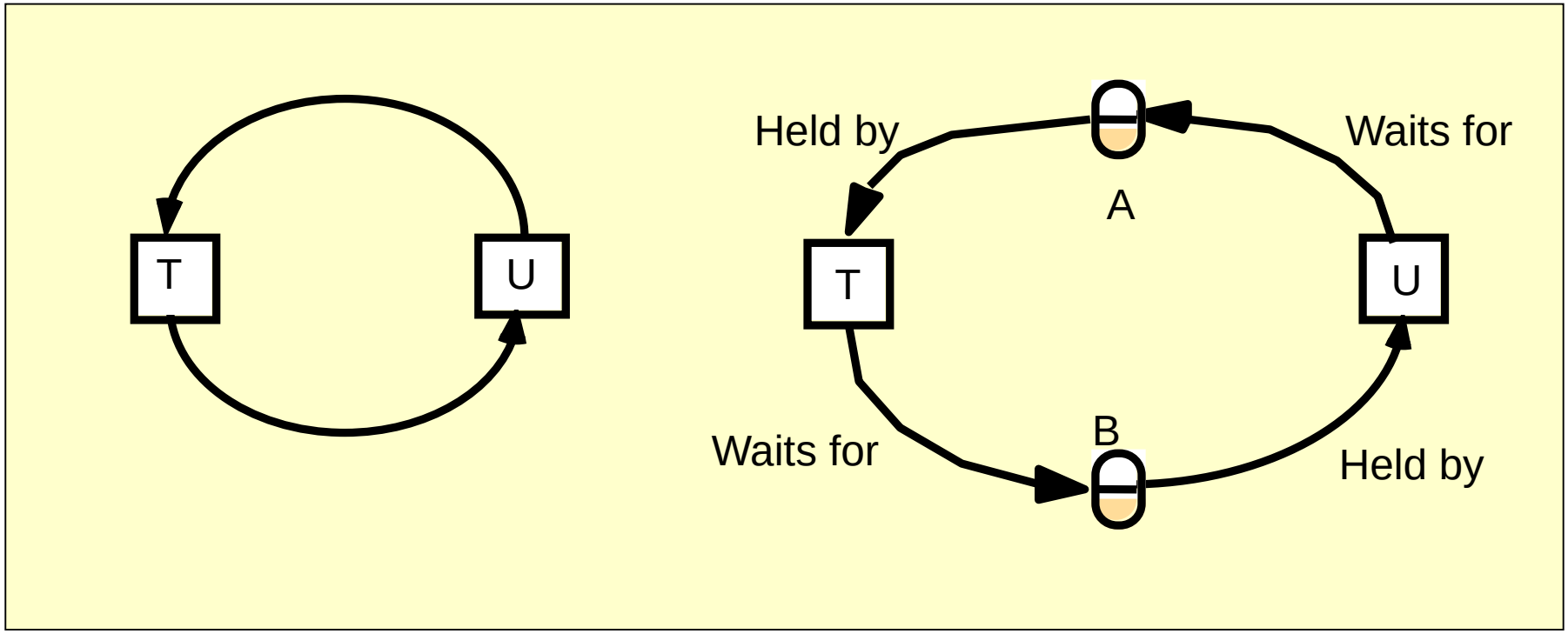
Transaction *T*		Transaction *U*	
Operations	**Locks**	**Operations**	**Locks**
a.deposit(100);	write lock *A*		
		b.deposit(200)	write lock *B*
b.withdraw(100)			
• • •	waits for *U*'s	*a.withdraw(200);*	waits for *T*'s
	lock on *B*	• • •	lock on *A*
• • •		• • •	
• • •		• • •	



T locks A and waits for U to release the lock on B, U on the other hand locks B and waits for T to release the lock on A

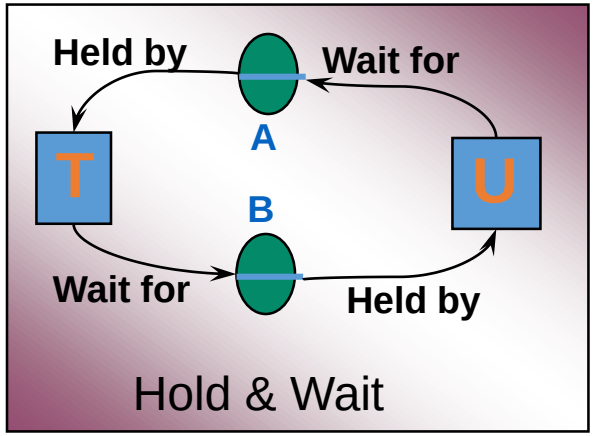
➔ Circular hold and wait ➔ Deadlock

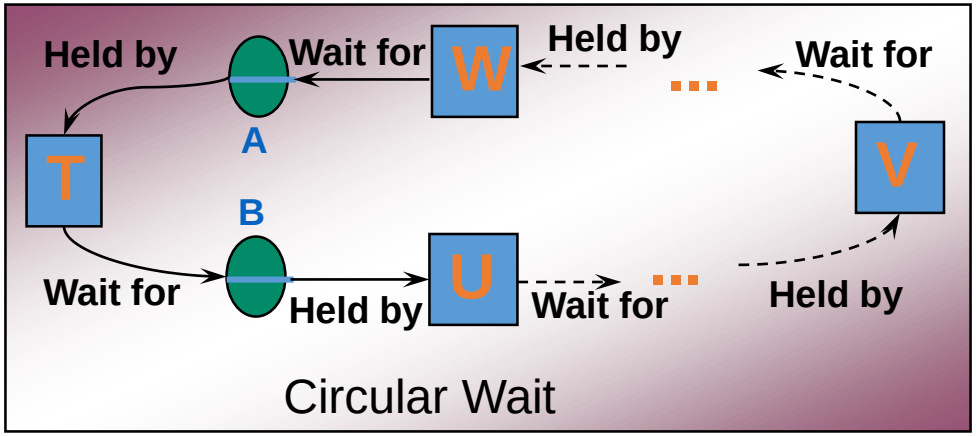
The corresponding wait-for graph



Deadlocks

- Necessary conditions for deadlocks
  - Non-shareable resources (exclusive lock modes)
  - No preemption on locks
  - Hold & Wait or Circular Wait





Naïve Deadlock Resolution Using Timeout

Transaction T		Transaction U	
Operations	**Locks**	**Operations**	**Locks**
a.deposit(100);	write lock *A*		
		b.deposit(200)	write lock *B*
b.withdraw(100)			
•••	waits for *U*'s lock on *B*	*a.withdraw(200);*	waits for T's lock on *A*
	(timeout elapses)	•••	
T's lock on *A* becomes vulnerable, unlock *A*, abort T		•••	
		a.withdraw(200);	write locks *A* unlock *A*, *B*

Disadvantages?

Strategies to Fight Deadlock

- Lock timeout (costly and open to false positives)
- Deadlock Prevention: violate one of the necessary conditions for deadlock (from 2 slides ago), e.g., lock all objects before transaction starts, aborting entire transaction if any fails
- Deadlock Avoidance: Have transactions declare max resources they will request, but allow them to lock at any time (Banker's algorithm)
- Deadlock Detection: detect cycles in the wait-for graph, and then abort one or more of the transactions in cycle

Optimistic Concurrency Control

(Kung and Robinson)

- We have seen locking has some problems
- OCC based on the following simple idea:
  - Don’t worry about the conflicts, keep on doing whatever you’re doing, if there’s a problem worry about it later.

Optimistic Concurrency Control

(Kung and Robinson)

- Algorithm
  - Each transaction has the following phases
    - Working phase
      - Each transaction has a tentative version of each object that it updates
      - Tentative version allows the trans. to abort w/o affecting the object

Optimistic Concurrency Control

(Kung and Robinson)

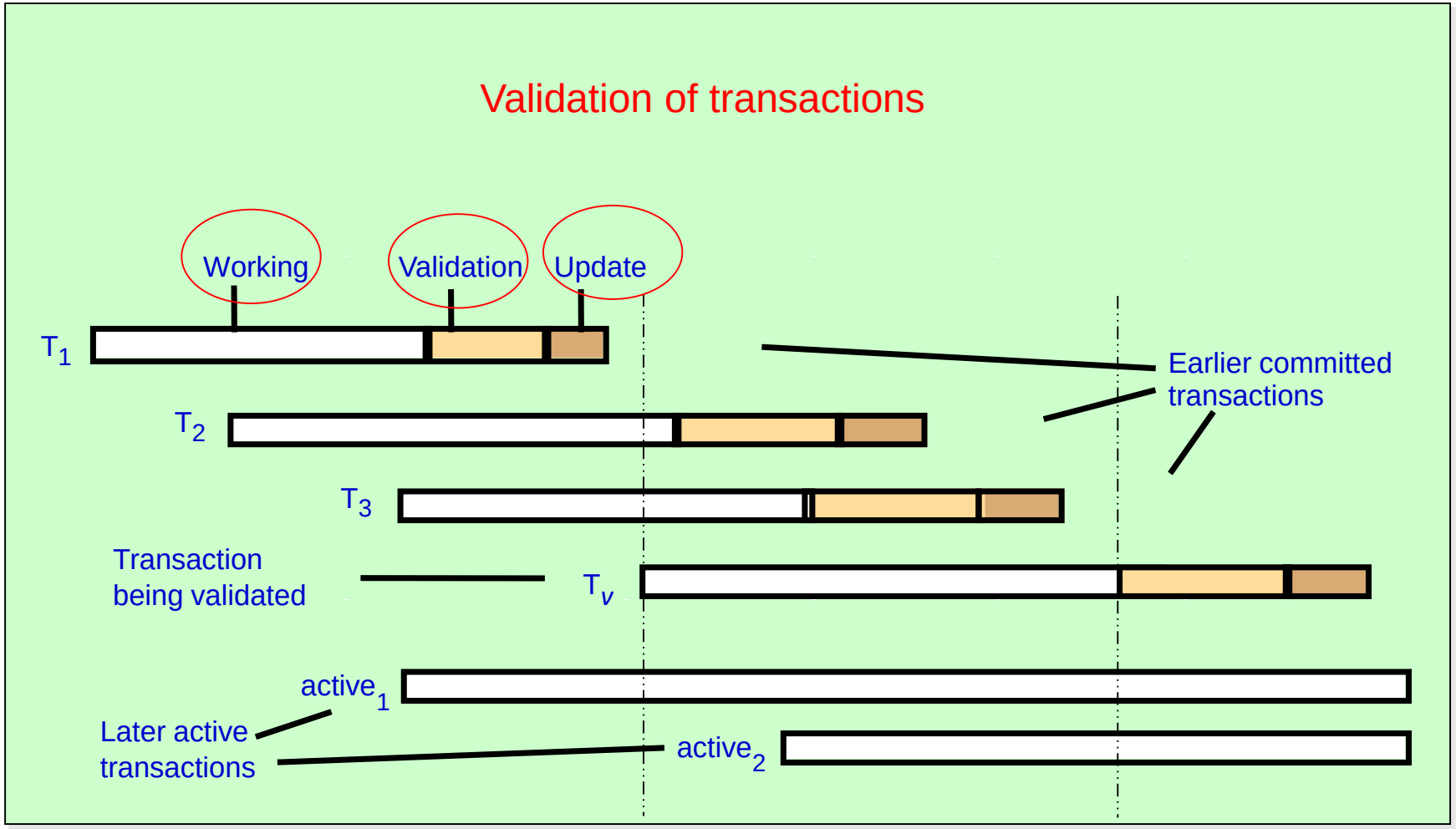
- Algorithm
  - Each transaction has the following phases
    - Validation phase
      - transaction is validated to see if any conflicts with other trans.

Optimistic Concurrency Control

(Kung and Robinson)

- Algorithm
  - Each transaction has the following phases
    - Update phase
      - if a trans. is validated all tentative objects are made permanent

Optimistic Concurrency Control:



Validation Rules

Tv	Ti	Rule
write	read	1. Ti must not read objects written by Tv
read	write	2. Tv must not read objects written by Ti
write	write	3. Ti must not write objects written by Tv and Tv must not write objects written by Ti

Validation of Transactions

Backward validation of transaction T_v

```
boolean valid = true;
for (int Ti  = startTn+1; Ti <= finishTn; Ti++){
        if (read set of Tv intersects write set of Ti) valid = false;
}
```

Forward validation of transaction T_v

```
boolean valid = true;
for (int Tid = active1; Tid <= activeN; Tid++){
        if (write set of Tv intersects read set of Tid) valid = false;
}
```

Solution

SMART DIGITAL IDENTITY

1 Connection

- Operates as a main hub that connects all devices together
- Connection of any smart device to another
- Additional hubs are not necessary

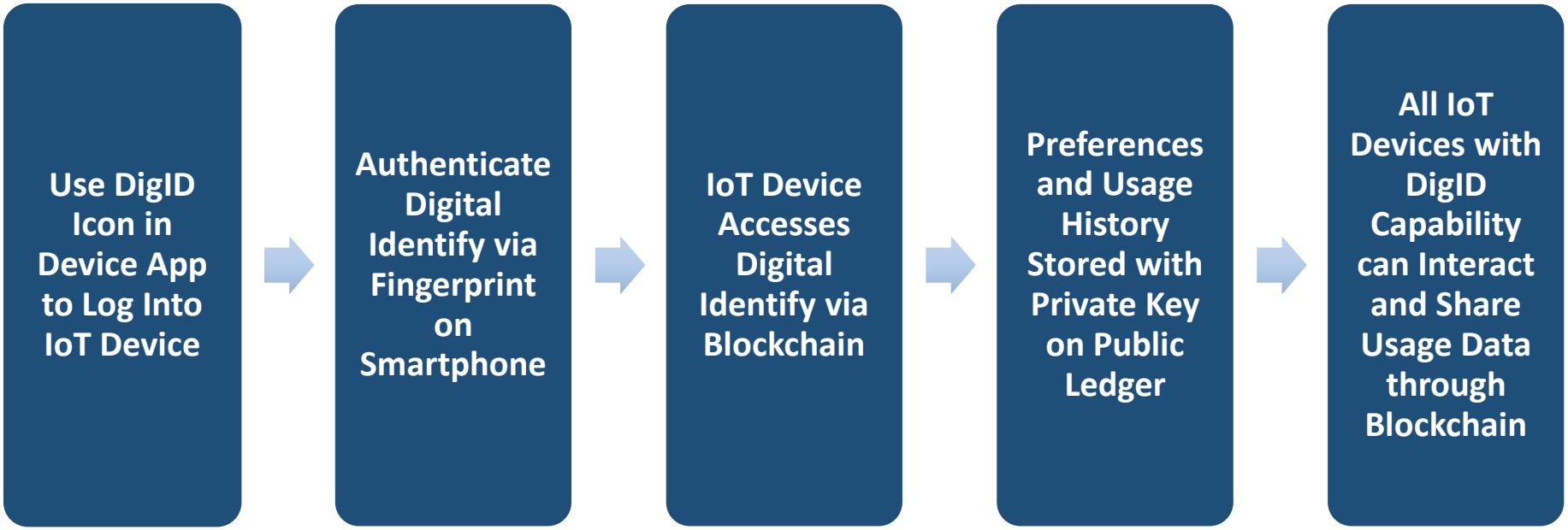
2 Efficiency

- Only one account (identity) that replace all online accounts
- Never use online passwords again
- Customized service based on the identity's preferences and history
- Reduce the costs associated with installing and maintaining large centralized data centers

3 Security

- Communications between devices go first through the digital identity and are executed as Blockchain transactions
- The Blockchain technology creates ledgers that are tamper-proof and cannot be manipulated
- Proven success in the world of financial services

Technology



- Separates usage information from user identity – usage information will be accessible to third party firms but will not be tied to any personally identifiable information
- Connects and integrates devices from different manufacturers
- Reduces complexity of manually connecting growing number of IoT devices

Technology

Value Proposition

One single control for all your smart devices, offer you a secure and worry free life

mind
for better mental health

Service Portfolio

Account Management

Risk Management

Business Model

Identity-as-a-Service (IDaaS)

Subscription based model
Unlimited number of connected devices for paid users

Addressable Market

By 2021, 13.5 million North American homes will have a professionally installed smart-home system.

Competitive Landscape

Enterprise: Mostly are B2B use cases (Okta)
Single platform focus (Apple HomeKit)
Startup: Blockstack, Civic, Uport, etc.

Go-to-market Strategy

Target Market

- Tech Savvy Millennials
- Home owners

Channel

- Direct sales
- White-label

Partnership

- OEMs: Google, Amazon, etc.
- Home builders
- Home insurance companies
- Cable & Telecom providers

Pricing

- “Freemium”: ten devices free
- Cost: technical integration of different devices

Competition

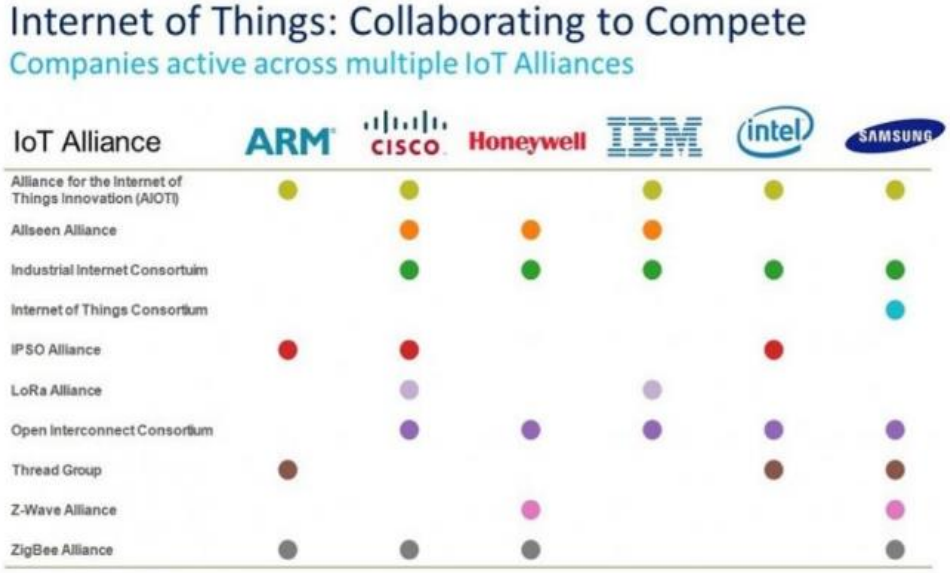
IoT is more than just a market, it's an entire ecosystem. Many competitors want a slice.

Promising Blockchain Identity Startups

Blockchain Identity Startups are building identity management applications for consumers to record and secure identification data

Giant Tech Companies

Giant Tech Companies are working on defining the standards for IoT and pairing it with the Blockchain technology



Challenges and Risks

1. Developing Collaborations and Partnerships in a Complex Environment

How can we get everyone to sign up when the business objectives of all parties of the business network are not completely aligned?

2. Low Processing Power of Current IoT Devices

Many IoT devices lack the significant horsepower needed for the encryption and verification of blockchain transactions.

3. Lack of Customers Awareness and Understanding

Blockchain is still in its early days and while many people are struggling to understand how it works; others don't even know that it exists.

Future Applications

This is only the tip of the iceberg!

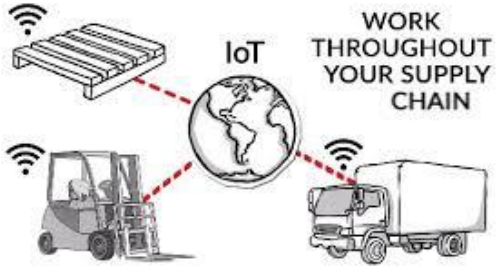
The idea is scalable to any IoT device – even those not yet in existence.

Possible targets for a Blockchain and IoT Pairing :

Smart Appliances

Connected Vehicles

Supply Chain Sensors



Future Applications - Examples

IMAGINE…

1. A refrigerator that autonomously manages its interactions with the external world – anything from placing orders from the grocery store and paying for food to downloading software upgrades and tracking its warranty
2. A connected car, smart enough to find and choose the best deal for parts and services

Reference

- The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous
- The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)
- Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial
- Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent
- Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)