FUJITSU

shaping tomorrow with you

Smart Contracts for Machine-to-Machine Communication: Possibilities and Limitations

Yuichi Hanada*, Luke Hsiao, and Philip Levis****

*Fujitsu Laboratories Ltd., **Stanford University

IoTaIS 2018 @Bali, Indonesia

Introduction

FUJITSU

- **Internet of Things has potential to transform daily life**
  - IoT devices communicate, gather data, and interact with the physical world
  - Applications in healthcare, agriculture, transportation, etc.

- **Rely on Machine-to-Machine communication**
  - To automate tasks
  - To send commands
  - To distribute information

Challenges

- Transparency
- Longevity
- Trust

Challenges

- **Transparency**
- Longevity
- Trust

German parents told to destroy doll that can spy on children

German watchdog classifies My Friend Cayla doll as 'illegal espionage apparatus' and says shops and owners could face fines

▲ Jayla, aged four, plays with a My Friend Cayla doll in the Hamleys toy shop in London. Photograph: Rob Stothard/Getty Images

Germany's telecommunications watchdog has ordered parents to destroy or disable a "smart doll" because the toy can be used to illegally spy on children.

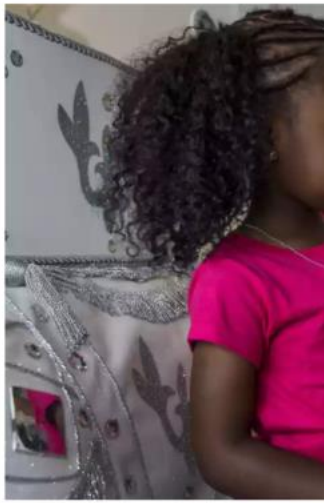
The My Friend Cayla doll, which is manufactured by the US company Genesis Toys and distributed in Europe by Guildford-based Vivid Toy Group, allows children to access the internet via speech recognition software, and to control the toy via an app.

Challenges

- **Transparency**
- Longevity
- Trust

German parents can spy on child

German watchdog classifies M espionage apparatus' and say



▲ Jayla, aged four, plays with a My Friend Ca Stothard/Getty Images

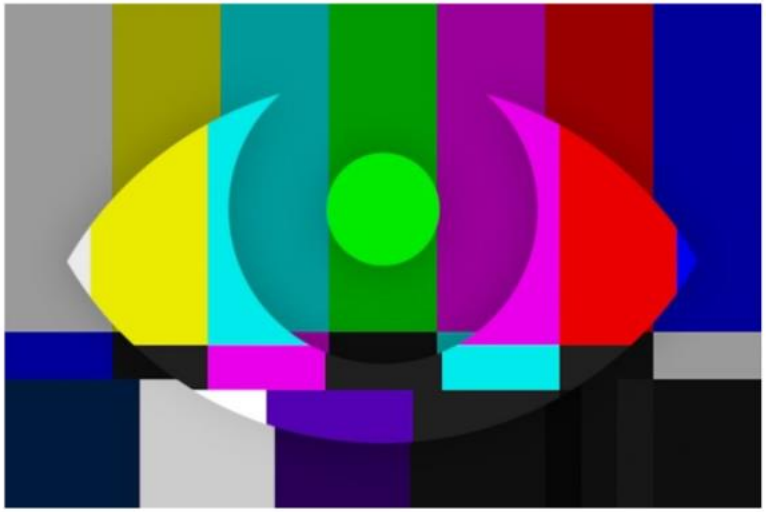
Germany's telecommunicatio disable a "smart doll" because children.

The My Friend Cayla doll, whi Genesis Toys and distributed i allows children to access the i control the toy via an app.

Own a Vizio Smart TV? It's Watching You

Vizio, one of the most popular brands on the market, is offering advertisers "highly specific viewing behavior data on a massive scale."

by Julia Angwin, Nov. 9, 2015, 12:57 p.m. EST



TV makers are constantly crowing about the tricks their smart TVs can do. But one of the most popular brands has a feature that it's not advertising: Vizio's Smart TVs track your viewing

Challenges

- Transparency
- **Longevity**
- Trust

Revolv devices bricked as Google's Nest shuts down smart home company

Customers furious as Nest is set to turn off Revolv units in just over a month

▲ Revolv was acquired by Google in 2014. Photograph: Revolv

Google owner Alphabet's subsidiary Nest is closing a smart-home company it bought less than two years ago, leaving customers' devices useless as of May.

In 2014, Google acquired Revolv, the maker of a £210 hub which could be used to control devices such as lights, alarms and doors.

The company was merged in with the wider team at Nest, Google's smart home subsidiary, and it immediately stopped selling its flagship device.

Challenges

- Transparency
- **Longevity**
- Trust

Revolv devices
shuts down sm

**Customers furious as Nest is
over a month**

▲ Revolv was acquired by Google in 2014.

Google owner Alphabet's sub
bought less than two years a

In 2014, Google acquired Re
used to control devices such

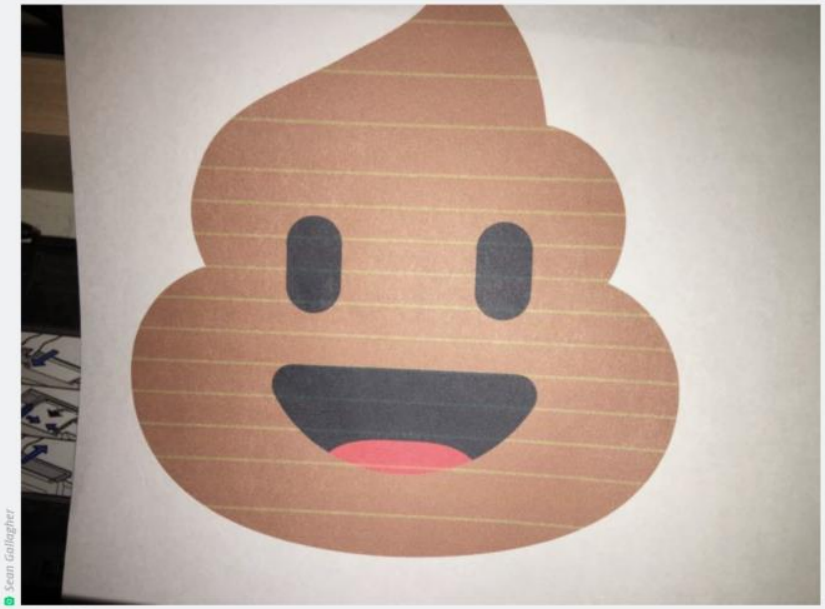
The company was merged in
home subsidiary, and it imm

BIZ & IT —

Internet of $@!%: Google API change triggers Epson printer revolt

Printers caught in reboot loop after API change causes firmware fail.

SEAN GALLAGHER - 12/9/2016, 12:51 AM



Sean Gallagher

Enlarge / Oh, poop.

Owners of Epson WorkForce, WorkForce Pro, and XP Series printers recently got a rude surprise, as the printers got stuck in a perpetual restart loop. And it quickly became apparent that the cause had something to do with the printers' connection to the Internet.

On the BleepingComputer boards, one Epson owner reported, "Yesterday it just turned off. I'd turn it back on and 30 seconds later it would turn off. I started messing around and turned off my router. The printer stayed on when I powered it up. Turned on my router and as soon as the printer connected to Wi-Fi it would turn off. I'd leave my router on and I disabled Wi-Fi on the printer and the printer stayed on."

Others reported similar experiences.

The affected printers all had one thing in common—they were connected to the Google Cloud

Challenges

- Transparency
- Longevity
- **Trust**

Facebook says data breach affected 29 million users

By Munsif Vengattil and Paresh Dave
Oct 15 2018
6:50AM

0 Comments

Cyber attackers stole data from 29 million Facebook accounts using an automated program that moved from one friend to the next, Facebook announced on Friday, as the social media company said its largest-ever data theft hit fewer than the 50 million profiles it initially reported.

The company said it would message affected users over the coming days to tell them what type of information had been accessed in the attack.

The breach has left users more vulnerable to targeted phishing attacks and could deepen unease about posting to a service whose

Emergent Tech ▸ Internet of Things

Wi-Fi baby heart monitor may have the worst IoT security of 2016

Gaping security holes, but a fix may be coming for Owlet

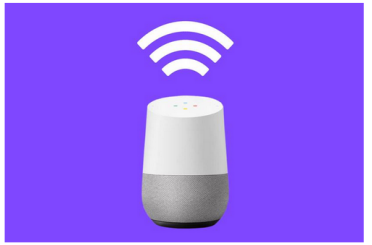
By Iain Thomson in San Francisco 13 Oct 2016 at 23:26 45 SHARE ▾

Not long ago, top computer security researcher Jonathan Zdziarski was blessed with a new baby and did what a lot of parents do – spent money on gizmos to keep an eye on it.

Google Home's data leak proves the IoT is still deeply flawed

Tripwire security researchers found the Google Home and Google Chromecast could leak location data through unauthorised network connections. The IoT's security issues run much deeper

By MATT BURGESS
Wednesday 20 June 2018



Credit: Google / WIRED / Artizarus

The Internet of Things (IoT) security problem isn't going away. The connected network of billions of devices – from smart doorbells to office printers – is regularly found to have privacy problems and be open to attack by potential hackers.

The latest of these incidents? Google's artificial intelligence Home speaker and the Chromecast, the firm's streaming device, have been found to reveal a user's precise physical location. Revealed by Tripwire security researcher Craig Young, the bug can make a person's location known to an accuracy of around 10 metres.

Contributions

FUJITSU

Blockchain technologies like Smart Contracts can address transparency, longevity, and trust

- **We present AGasP, an example IoT application that uses Smart Contracts for M2M communication**
- **Practical trade-offs: performance, privacy, and the impact of bugs**

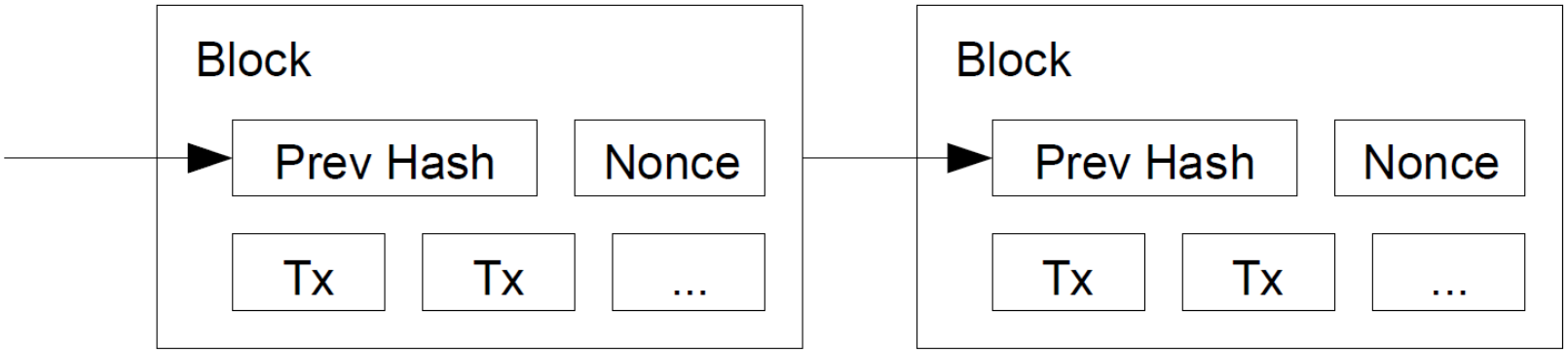
Background

- Blockchain
- Smart Contract
- Ethereum

Background

FUJITSU

- **Blockchain**
  - **Distributed management of ledger information in P2P network**
  - **Mechanism**
    - **Block has transactions**
    - **Blocks are connected by referring to the hash of previous block**



Reference: https://bitcoin.org/bitcoin.pdf

Background

- Blockchain
- **Smart Contract**
  - **Acts as an autonomous entity on the blockchain**
  - **Provides a way to deterministically execute programs**
- Ethereum

Background

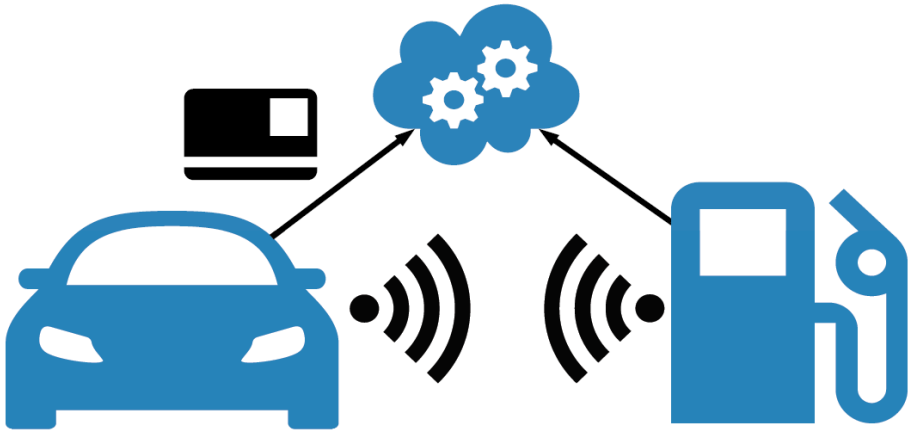
- Blockchain
- Smart Contract
- **Ethereum**
  - **Blockchain Platform that supports Smart Contracts**

An example application

FUJITSU

AGASP : Automated Gasoline Purchases

- **Traditional**
  - **Single vendor controls everything car to cloud**
  - **Users must trust the vendor with personal information**
    - **Credit card information**
    - **Location, etc.**

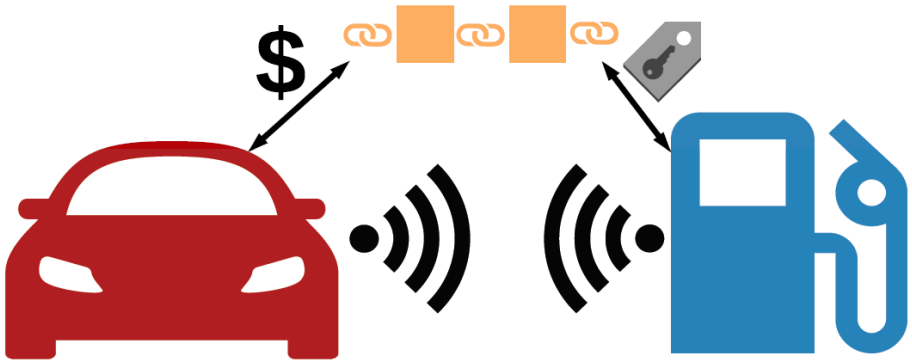


An example application

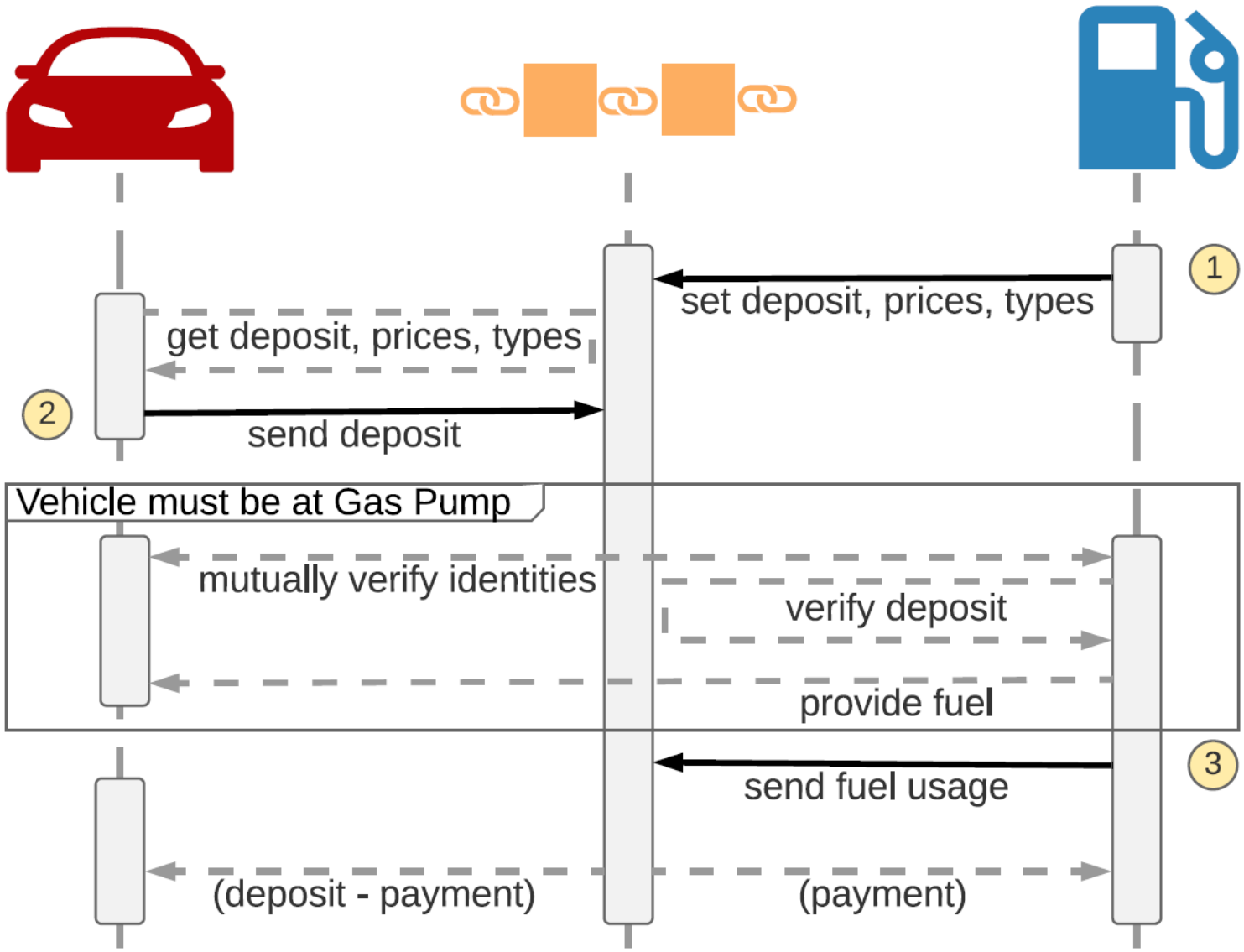
FUJITSU

AGASP : Automated Gasoline Payments

- **Our approach**
  - No single vendor controls all of the pieces
  - Pay for fuel by using Smart Contracts in Ethereum, rather than trusting a vendor with payment information
  - DApp (Decentralized Application) can interact directly with the public blockchain



AGAsP: Sequence



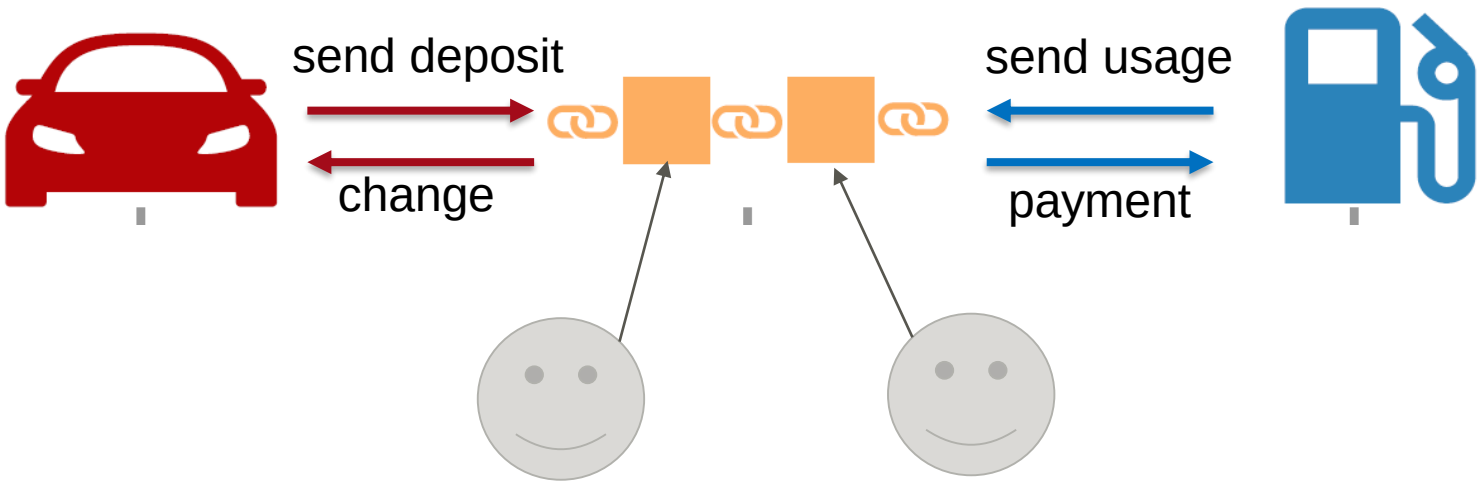
How does it address?

FUJITSU

- Transparency
- Longevity
- Trust

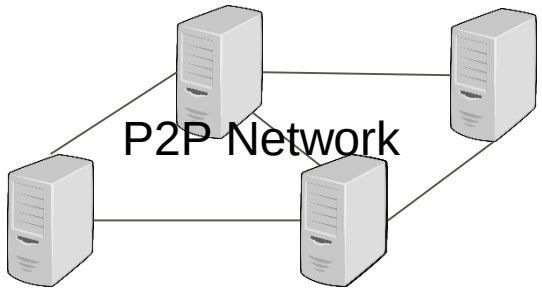
How does it address?

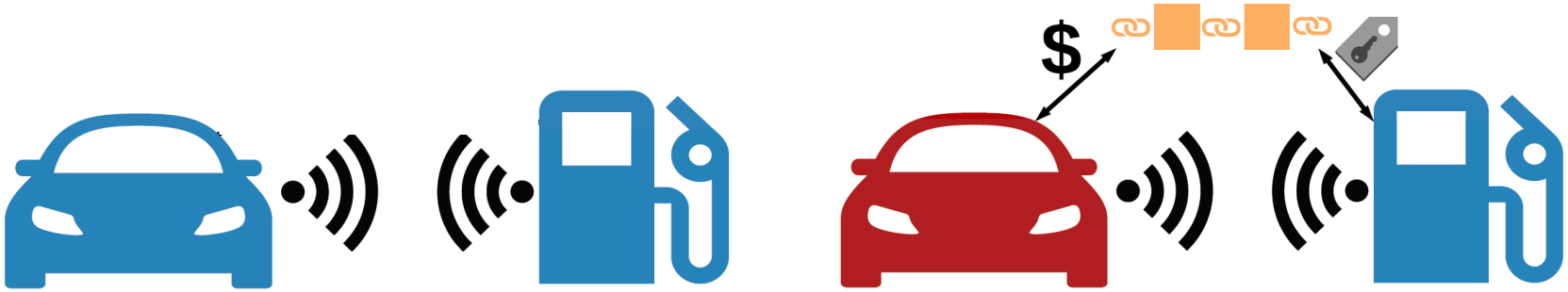
- **Transparency**
  - **Both the vehicle and pump MUST communicate through the blockchain**
- **Longevity**
- **Trust**



How does it address?

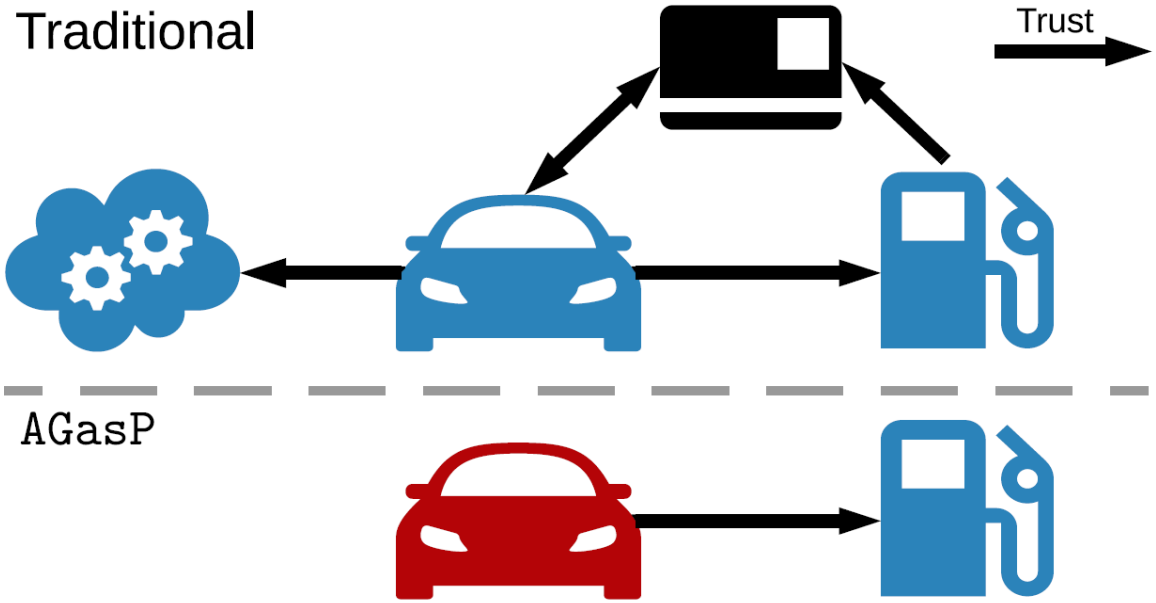
- Transparency
- **Longevity**
  - **Guarantee permanence of infrastructure and application**
    - **Based on the permanence of the Ethereum network.**
    - **Set up new Ethereum nodes**
- Trust





How does it address?

- Transparency
- Longevity
- **Trust**
  - **Reduce the relation of trust to just a single edge**



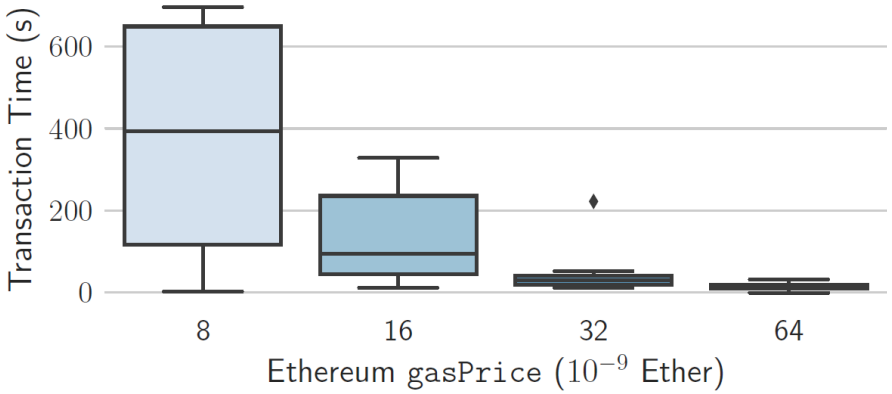
Comes with limitations

FUJITSU

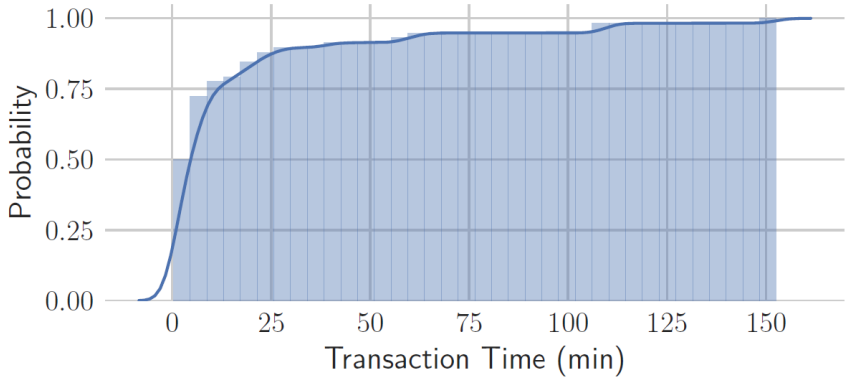
- Performance
- Privacy
- Impact of bugs in Smart Contract

Comes with limitations

- **Performance**
  - **Transactions have high latency and are heavily influenced by fees (Ethereum gasPrice)**
- **Privacy**



Transaction Time is significantly affected by gasPrice



Transaction time has long 95% latency for a fixed gasPrice

Applications must be designed around long latencies

Comes with limitations

FUJITSU

- Performance
- **Privacy**
  - **Transactions are publically viewable, which can leak personal information**
  - **Need methods to mask information while remaining auditable**
    - **zero-knowledge Succinct Non-interactive ARguments of Knowledge (zkSNARK)**
    - **Hawk**
- Impact of bugs in Smart Contract

Applications should protect user privacy while remaining auditable

Comes with limitations

FUJITSU

- Performance
- Privacy
- **Impact of bugs in Smart Contract**
  - **Smart contract contains critical flaws**
    - **logical errors**
    - **lack a self-destruct**
  - **Assets can be locked in a contract**

Press release: **Fujitsu Develops Technology to Verify Blockchain Risks**
Risk detection is automatic and comprehensive to improve safety of smart contracts
2018.3.7 Fujitsu Laboratories Ltd., FRDC in China

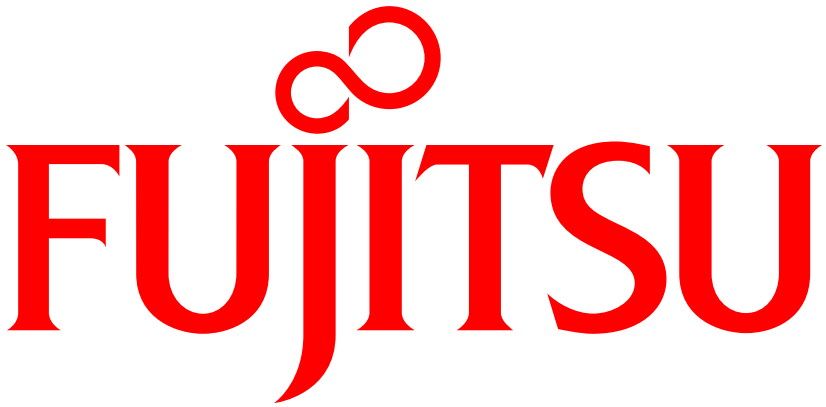
Future work on developer tools and static analysis can prevent large classes of vulerabilities or logical errors

Conclusion

FUJITSU

- **We highlight challenges of Transparency, Longevity, and Trust for IoT applications.**
- **We perform an initial exploration of using smart contracts as a solution by designing, implementing, and evaluating AGasP on the Ethereum blockchain.**
- **We discuss the potential limitations of performance, privacy, and the impact of bugs in the context of machine-to-machine communication.**

Thank you for your attention. Terima Kasih!!



shaping tomorrow with you