101 Blockchains Think Tank Webinar Series

LIVE WEBINAR

101 Blockchains

Confidential Computing: It Promises to be the 'Big Thing' of 2021 but what is it?!

Presented by:

Richard G. Brown
Chief Technology Officer, R3

r3

101 Blockchains Think Tank Webinar Series

LIVE WEBINAR

101 Blockchains

Confidential Computing: It Promises to be the 'Big Thing' of 2021 but what is it?!

- Analyze data from multiple parties in a protected algorithm, and verify how data is used.
- Protect customer data from misuse and provide assurance that the data remains protected when collected, shared and analyzed.
- Access previously inaccessible customer data to deliver new insights and AI without compromising on confidentiality.

Presented by:

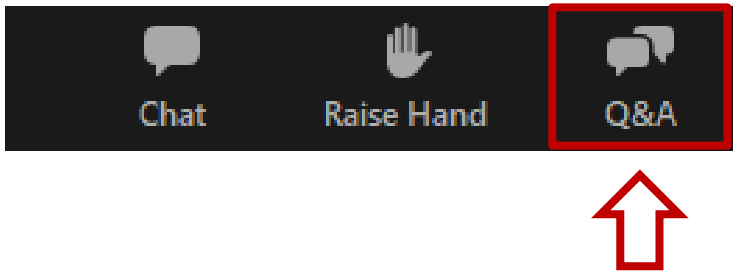
Richard G. Brown
Chief Technology Officer, R3

r3.

A few housekeeping tips

101 Blockchains

Use the **Q&A** tab to ask your questions



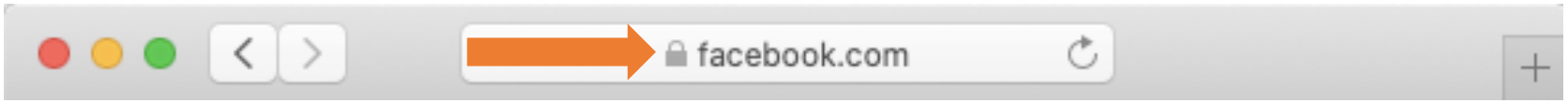
Webinar Partner: r3.

Introduction to Confidential Computing

Richard G Brown

Chief Technology Officer, R3

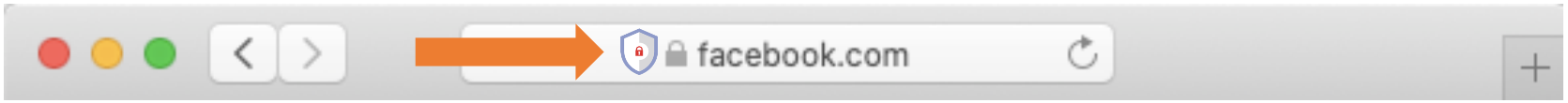
Current state:



✅ You know who you're talking to

❌ You don't know what they're doing with your data

Future state:



conclave

✅ You know who you're talking to

✅ You **DO** know what they're doing with your data

r3.

Example: Confidential Auction

Problem: you want to run a private and tamperproof auction where no bids can be viewed or tampered with by auction host

Challenge: no technological way to prove data is not misused or tampered with by the host

Solution: use Conclave to prove data is protected and auction results cannot be tampered with

Privacy Policy

This application receives buy and sell offers.

The service operator can see:

- When you submit an order
- Who is submitting orders
- When a trade matches

The service operator cannot see:

- The contents of an order
- The contents of a trade

The policy was checked automatically and is being enforced.

Confidential Computing: Protecting Data in Use

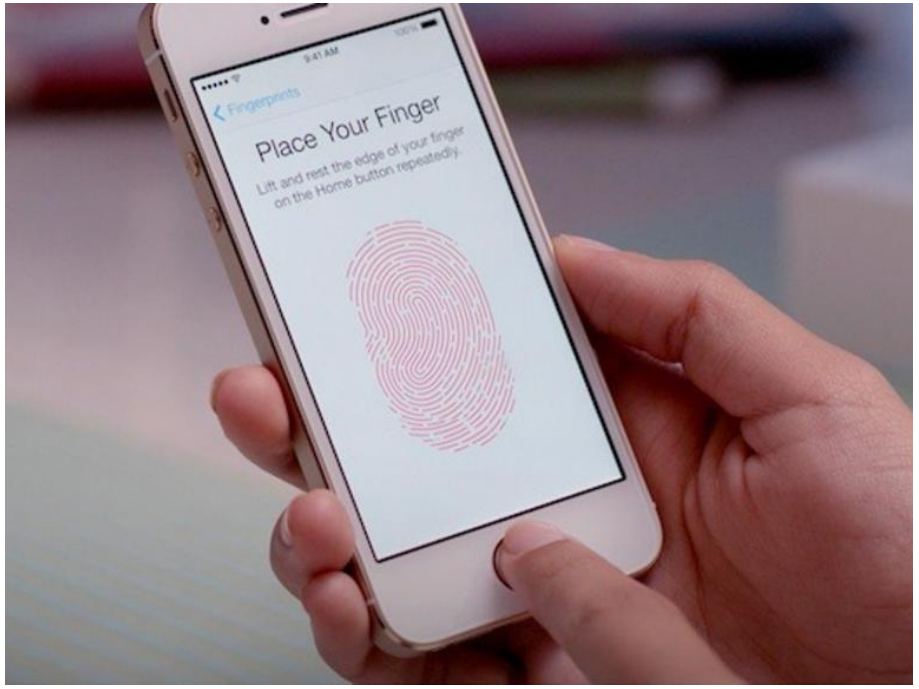
Confidential Computing *provides assurances to users that data is processed as described and in a tamperproof way.*

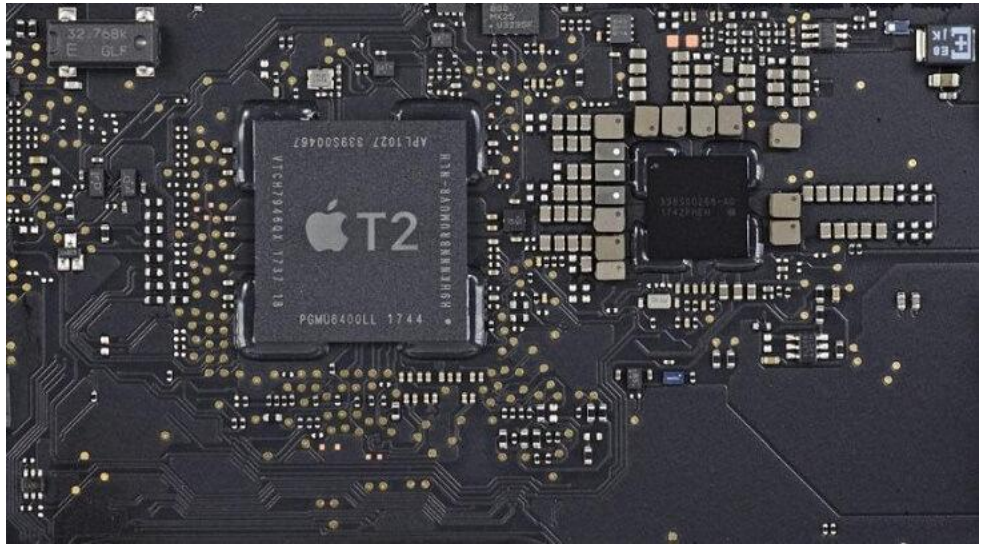
EXISTING ENCRYPTION		NEW
		
Data at rest	**Data in transit**	**In use**
Encrypt inactive data when stored in blob storage, database, etc.	Encrypt data that is flowing between untrusted public or private networks	Protect/Encrypt data that is in use, while in RAM and during computation.

R3's Conclave is an example of a Confidential Computing platform, based on Intel SGX

Image source: Confidential Computing Consortium

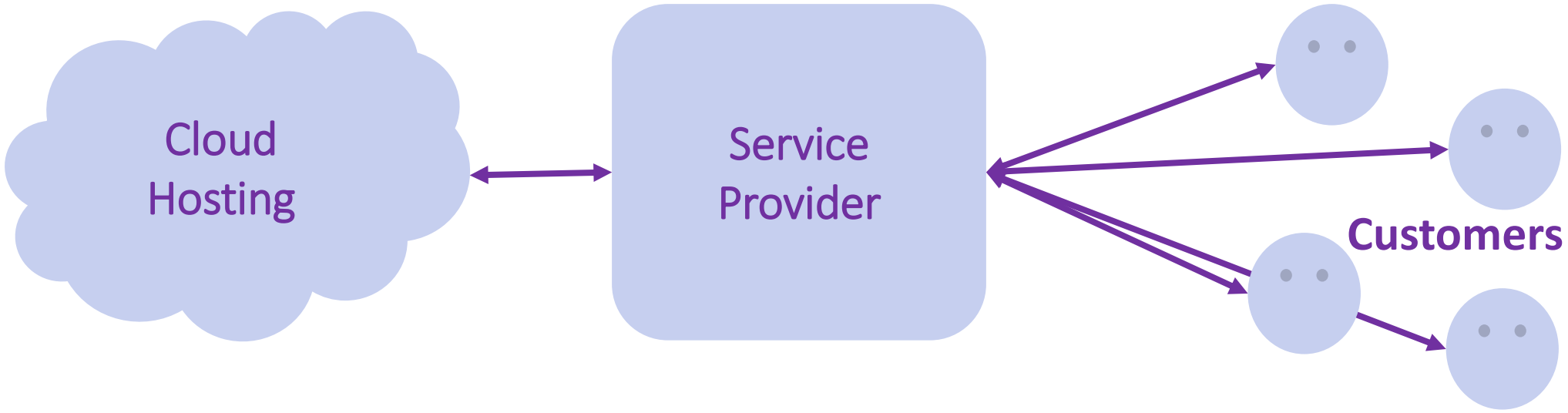
Confidential Computing is not new





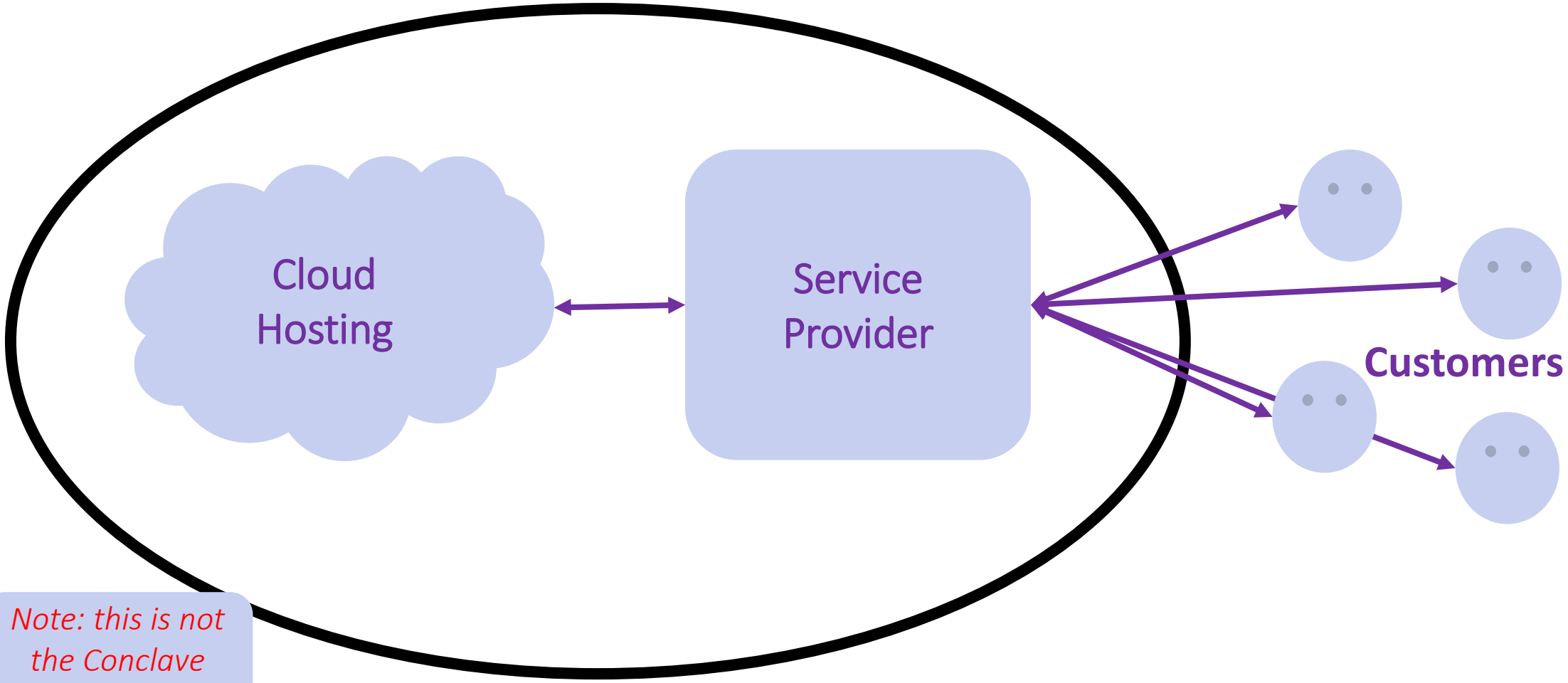
We see two distinct use-cases for Confidential Computing

R3 is focused on one of them, where we believe we can strongly differentiate



Confidential Computing Use-Case 1:

Securing VMs in the cloud – "Protect the ISV from the cloud vendor"



Note: this is not the Conclave target market

Confidential Computing Use-Case 1:

Securing VMs in the cloud – "Protect the ISV from the cloud vendor"

Google Cloud Confidential VMs and IBM Cloud Hyper Protect Virtual servers **protect applications in use:**

- Prevents cloud administrators from accessing the data
- Sales pitch: "does not require code change to applications"
  - *Note: likely that **some** modifications needed to mitigate all threats*

Note: this is not the Conclave target market

Introducing Google Cloud Confidential Computing with Confidential VMs

IBM Cloud Hyper Protect Virtual Servers

Gain complete authority over workloads with sensitive data or your business IP

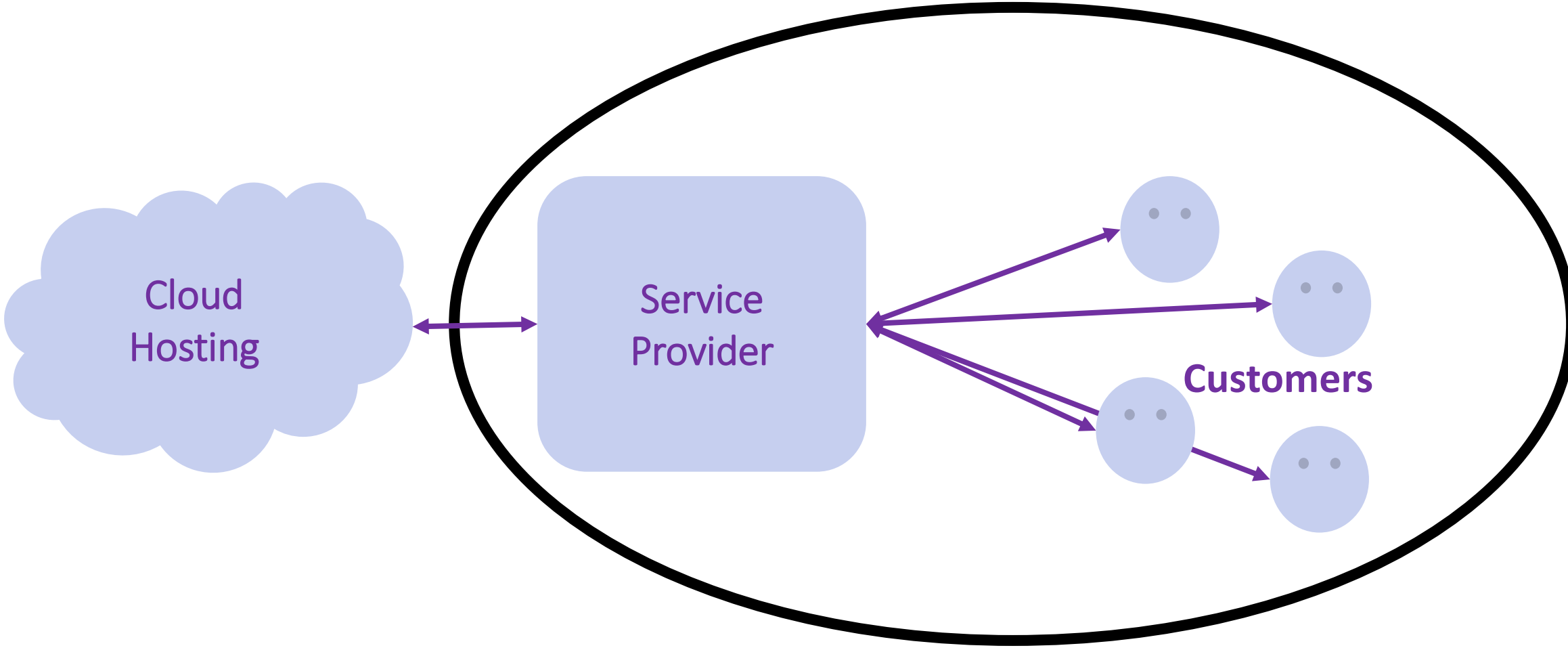
IBM, R3 team up to bring blockchain technology to hybrid cloud deployments

ZDNet

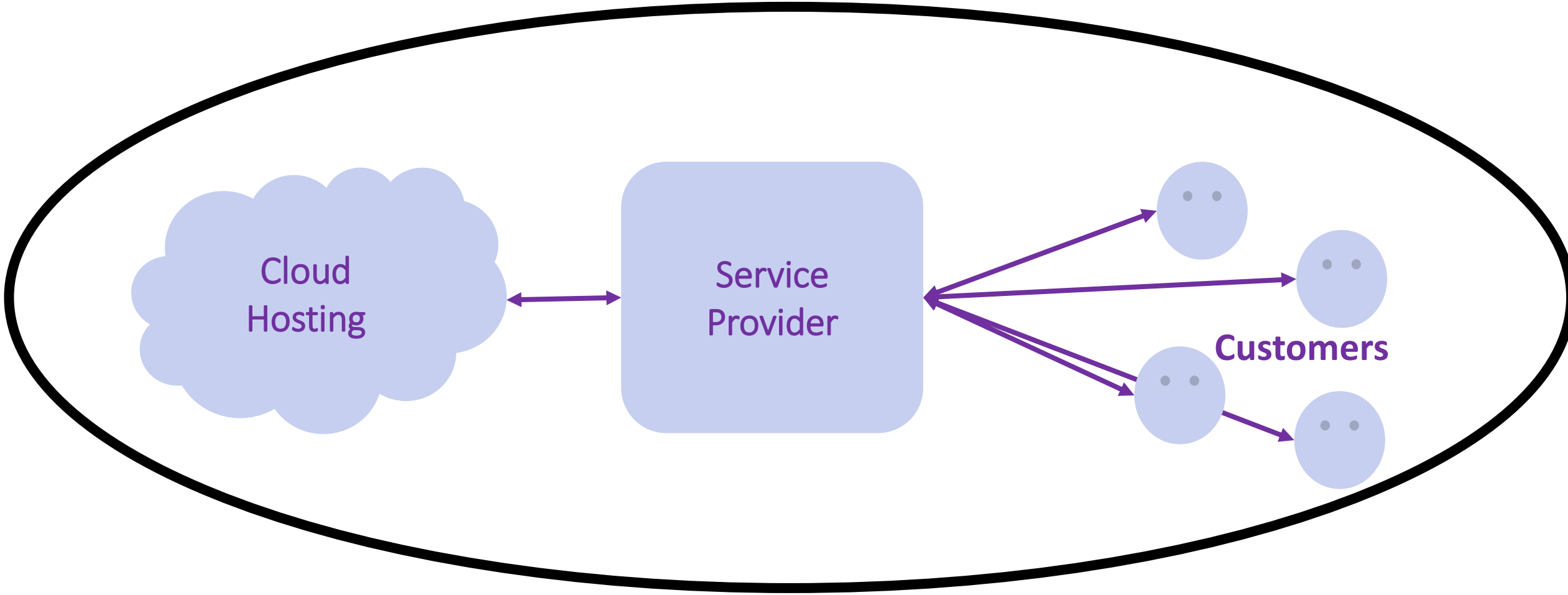
r3.

Confidential Computing Use-Case 2:

Apps that prove what they do: "Protect the customer from the service provider"



Confidential Computing Use-Case #2 expands to protect customers from the service provider and cloud vendors



Recall: Confidential Auction

This is an example of "protect the customer from the service provider"

Problem: you want to run a private and tamperproof auction where no bids can be viewed or tampered with by auction host

Challenge: no technological way to prove data is not misused or tampered with by the host

Solution: Use Confidential Computing to prove data is protected and auction results cannot be tampered with

Privacy Policy

This application receives buy and sell offers.

The service operator can see:

- When you submit an order
- Who is submitting orders
- When a trade matches

The service operator cannot see:

- The contents of an order
- The contents of a trade

The policy was checked automatically and is being enforced.

Confidential Computing is primarily a hardware story

But it needs software to make it mainstream

How do we protect a customer from their service provider?

- Confidential Computing hardware technologies like Intel SGX allow programs to run inside a “secure enclave” that **protects data from the operator of the system**
- And some such platforms (Intel SGX, notably) can then **prove** to users what algorithm is running and hence how their data will be used

Why is this valuable? Corporates can be confident sensitive data will only be used for purposes agreed upfront and **can not be viewed or misused** even if the service provider – or an employee – goes rogue

But there's a catch: It's extremely difficult to use! Enter **Conclave**…

r3.

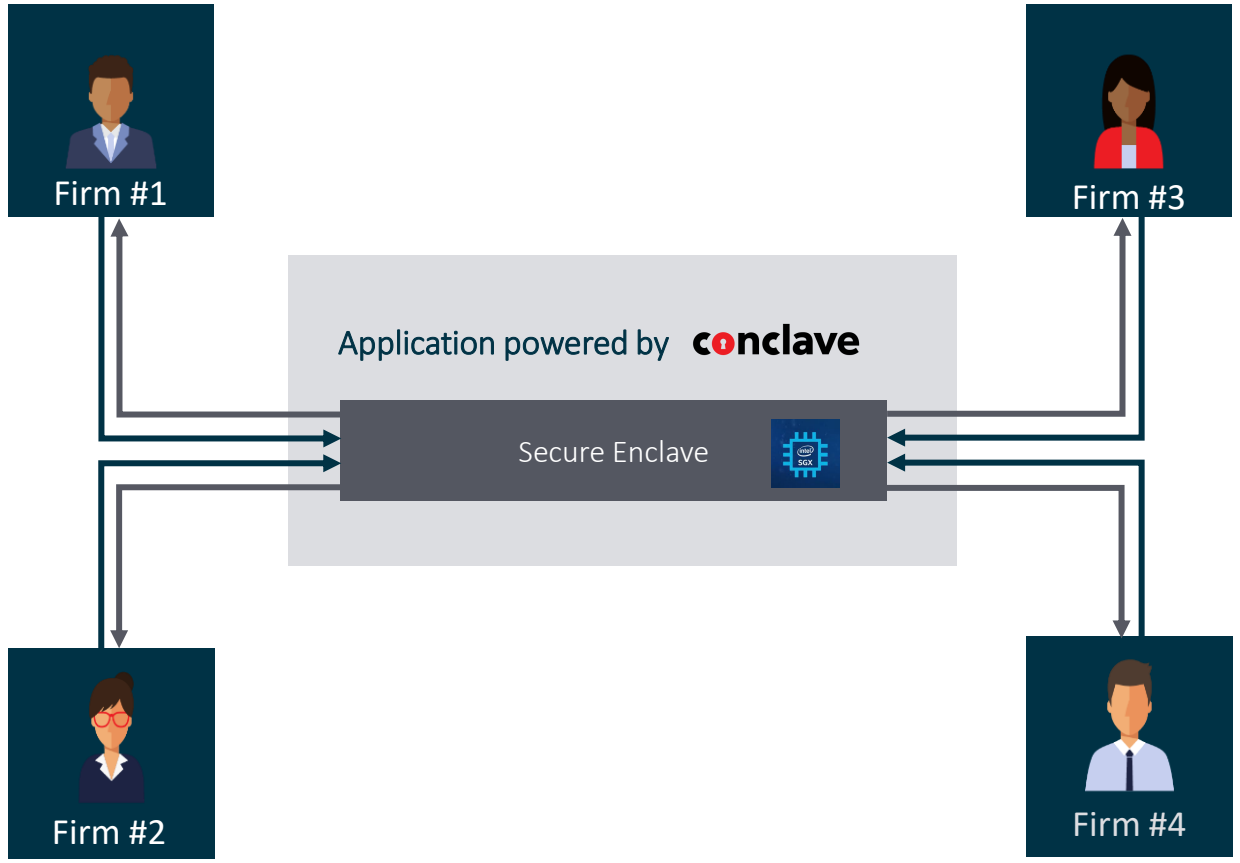
conclave - A platform to securely share and analyze data

Feature	Benefit
 Developer-friendly	Easy to use
 Java-based	Productive
 Focus on business logic	Reduced time to value
 Integration with CE	Robust multi-party solutions

Conclave makes Confidential Computing accessible to Enterprises to solve pressing business problems

What is now possible:

- Corporates can now **share sensitive data** with counterparties, competitors and service providers with confidence it **will not be viewed or tampered with**
- ISVs and corporates can **protect customers from data misuse** in a technologically-backed way
- Service providers can **aggregate sensitive data** to provide new solutions or insights **without revealing underlying data sets**



Conclave solves pressing Business Problems for Service Providers and Corporates

Financial Crime and AML vendors

Solve for Cross-Institutional Fraud Detection, Anti-Money Laundering, Financial Crime

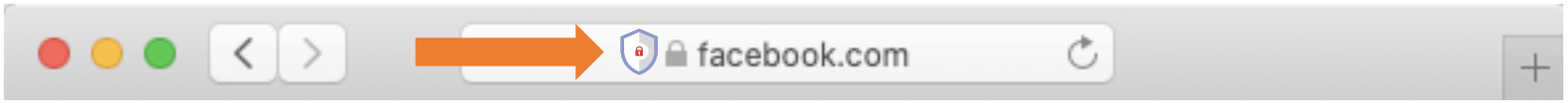
AI / ML and Analytics companies

Train or deploy models with previously inaccessible sensitive data

FMIs, Data Vendors, and Banks

Private Order Matching, Dark Pools, Market Data, Benchmarking

Future state:



conclave

✅ You know who you're talking to

✅ You **DO** know what they're doing with your data

Find out more at conclave.net

r3.

Thank you

www.r3.com | corda.net

linkedin.com/company/r3cev-llc

@inside_r3 | @cordablockchain

Headquarters:

New York
11 West 42nd Street, 8th Floor
New York, NY 10036

London
2 London Wall Place,
London, EC2Y 5AU

Regional:

Dublin
Lennox Building
50 Richmond St South
Saint Kevin's, Dublin, D02FK02

Hong Kong
Bonham Strand, 7F Office 18-121
Hong Kong

Mumbai
01A108, WeWork Enam Samhav, C-20, G Block, Bandra Kurla Complex,
Mumbai, 400051, India

San Francisco
655 Montgomery St., 6th floor
San Francisco, CA 94111

São Paulo
Av. Angélica, 2529
Bela Vista- 6th Floor
São Paulo - SP, 01227-200, Brazil

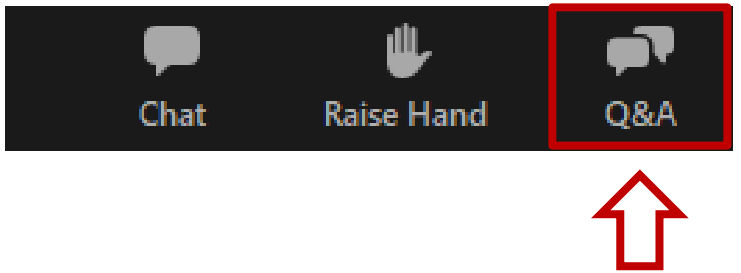
Singapore
18 Robinson Road, Level #14-02
Singapore, 048547

Tokyo
Izumi Garden Tower 19F,
1–6-1 Roppongi, Minato-ku,
Tokyo 106-6019, JAPAN

Q&A time

101 Blockchains

Use the **Q&A** tab to ask your questions



Webinar Partner: r3.

Poll

Do you plan to explore Confidential Computing technology in 2021?

- Immediately
- Within the next 3-6 months
- Within the next 6-12 months
- No plans to explore

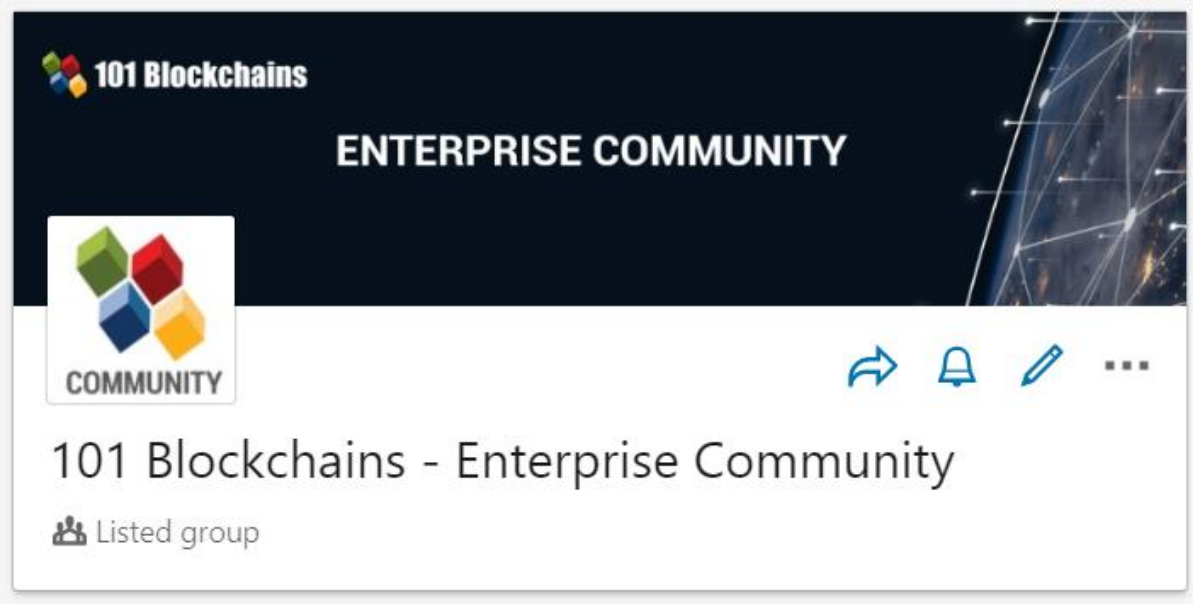
Poll

What are your drivers to justify Confidential Computing spending?

- Increased data protection
- Support of regulatory initiatives
- Protect data from cloud vendor
- Build and sell tamperproof services
- Net new revenue generation
- Other

Join our Group on LinkedIn

https://www.linkedin.com/groups/12400295/



ARE YOU READY TO JOIN THE BLOCKCHAIN REVOLUTION?

101 Blockchains

- 101blockchains.com
- contact@101blockchains.com
- linkedin.com/company/101blockchains
- https://www.linkedin.com/groups/12400295/