Keynote II

서상민 / Ground X

Challenges for Blockchain Mass Adoption

서상민, Sam,
Ph.D.

Head of Tech, Ground X

- Leading the development of Klaytn, SDK, toolkits and services

Senior Engineer, Samsung Research

- Neural network inference framework for on-device AI
- Tizen toolchain development

Assistant Computer Scientist, Argonne National Lab.

- MPICH: A High-Performance, Portable Implementation of the MPI Standard
- ARGO: An Exascale Operating System and Runtime Research Project
- BOLT: OpenMP over Lightweight Threads

Ph.D. in Computer Science, Seoul National University

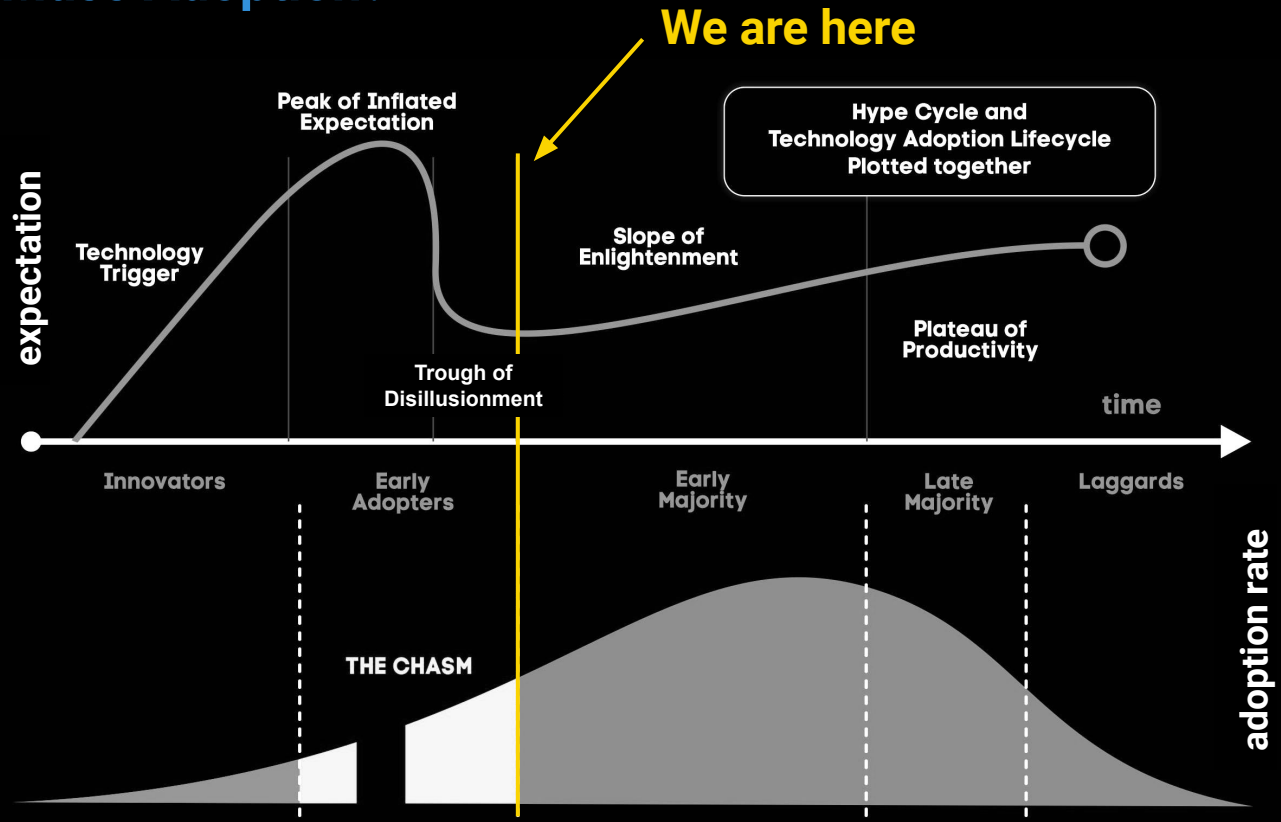
- Performance optimizations of parallel programming models on heterogeneous multicore architectures

GROUND X Copyright © Ground X. All rights reserved.

Are We Using Blockchains in Everyday Life?

GROUND X Copyright © Ground X. All rights reserved.

Blockchain Mass Adoption?



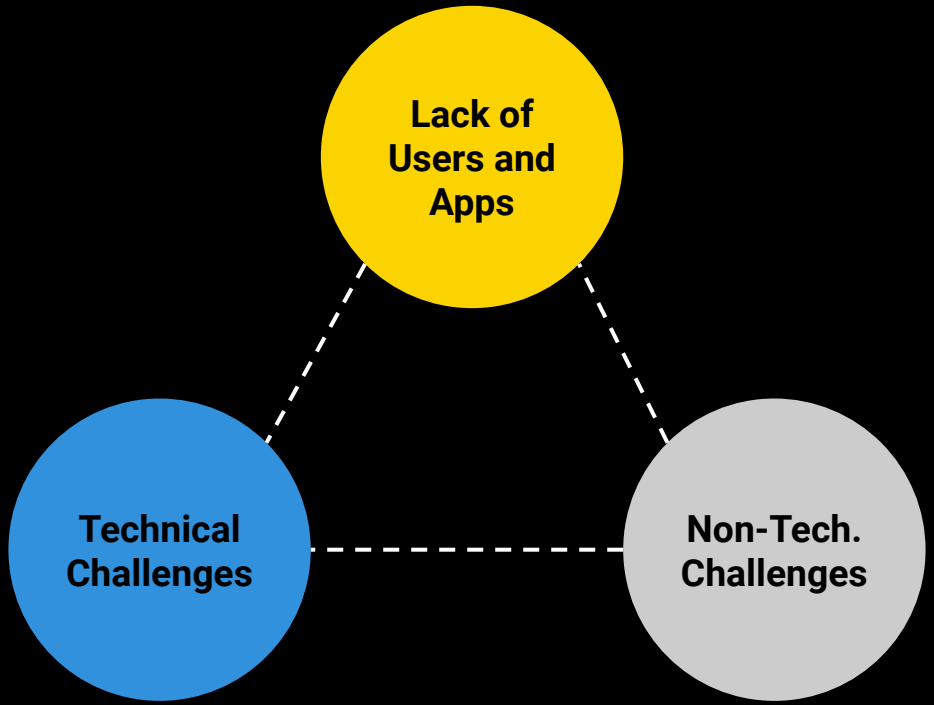
source: https://medium.com/tozex/application-of-the-diffusion-of-innovation-theory-to-blockchain-technology-b4d9535507fa

GROUND X Copyright © Ground X. All rights reserved.

Challenges for Blockchain Mass Adoption

GROUND X Copyright © Ground X. All rights reserved.

Challenges for Blockchain Mass Adoption



- Performance
- Scalability
- Interoperability
- Security & Privacy
- Ease of Use & Development
- ...

- Public Perception
- Regulation
- Lack of Developers
- ...

GROUND X Copyright © Ground X. All rights reserved.

Lack of Users and Apps

GROUND X Copyright © Ground X. All rights reserved.

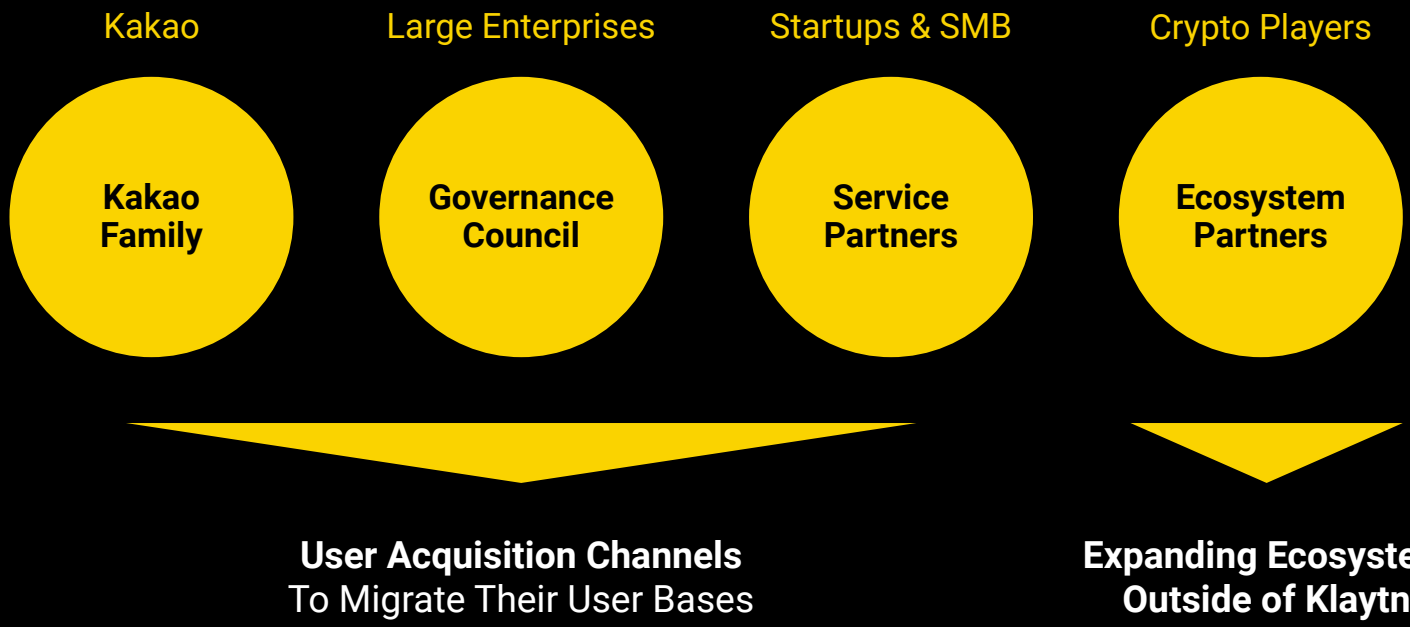
The State of Apps and Platforms

	Mobile Apps	Blockchain Apps
Number of APPS	~5.8 M	~2,000
Number of Users	~250 M	~2.4 M
Key Players		

GROUND X Copyright © Ground X. All rights reserved.

Building Practical Use Cases with Partners on Klaytn

Klaytn is adding more and more partners who have potentials to build their own blockchain apps and bring their existing users into Klaytn



GROUND X Copyright © Ground X. All rights reserved.

Klaytn on STATE OF THE ĐAPPS

Platforms

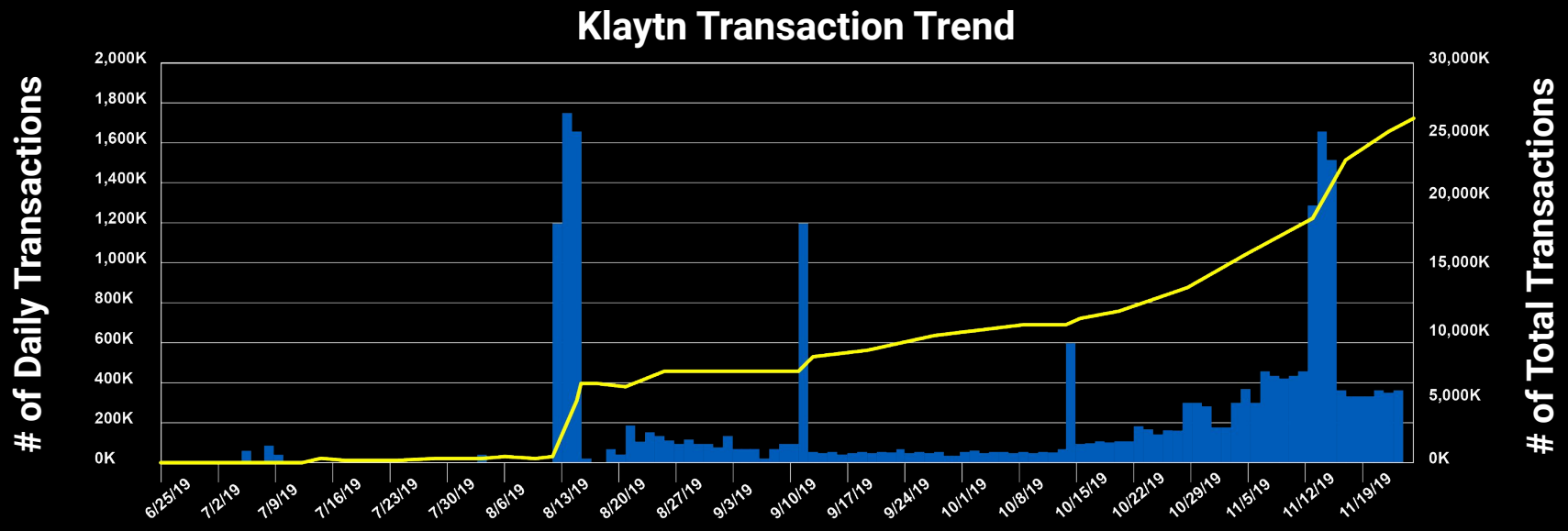
Platform	Total DApps	Daily active users	Transactions (24hr)	Volume (24hr)	# of contracts
Ethereum	2,690	23.04k	83.37k	189.98k	3.9k
EOS	313	11.44k	420.41k	334.39k	480
Steem	91	9.26k	325.65k	105.83k	160
Klaytn	21	40.55k	204.32k	0	53
POA	19	208	3.55k	0	48
NEO	17	1.85k	5.33k	0	25
xDai	12	5	7	0	39
Loom	10	?	?	?	70
GoChain	7	?	?	?	17
OST	2	54	694	17.31k	2

* Data collected on Nov. 25, 2019

GROUND X Copyright © Ground X. All rights reserved.

Klaytn Mainnet's Growth Rate

Since its launch in June 2019, Klaytn Mainnet successfully established rapid rate of adoption and growth by business entities



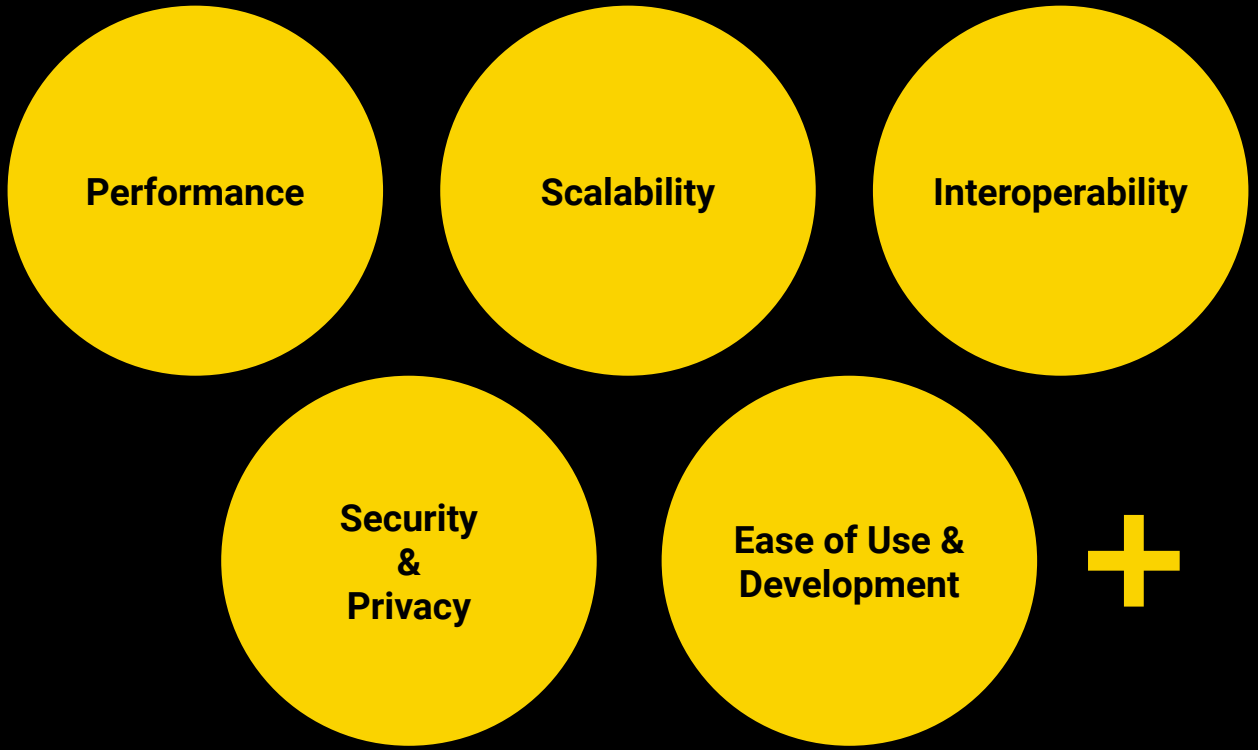
* Data range: June ~ November 2019

GROUND X Copyright © Ground X. All rights reserved.

Technical Challenges

GROUND X Copyright © Ground X. All rights reserved.

Technical Challenges



GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge I
Performance

GROUND X Copyright © Ground X. All rights reserved.

	Bitcoin	Ethereum	Ripple	EOS	Stellar
Time to finality	15 min	6 min	4 sec	180 sec	2-5 sec
Transactions per second (TPS)	7	15	1,500	3,000	1,000

Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. Logistics, Litke et. al. (2019).
https://medium.com/perlin-network/bite-sized-2-why-is-tps-time-to-finality-important-bd01baffdf05

GROUND X Copyright © Ground X. All rights reserved.

Klaytn Cypress Performance

Latency

1 sec

block interval

Enables mobile
app-like performance

Throughput

4,000

TPS

Supports production-grade
enterprise usage

GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge II
Scalability

GROUND X Copyright © Ground X. All rights reserved.

Scalable Performance on HPC

Nuri (Korea Meteorological Administration)

- **69,600 cores / 2.4 PFLOPS**
- #113 supercomputer (Nov. 2019)

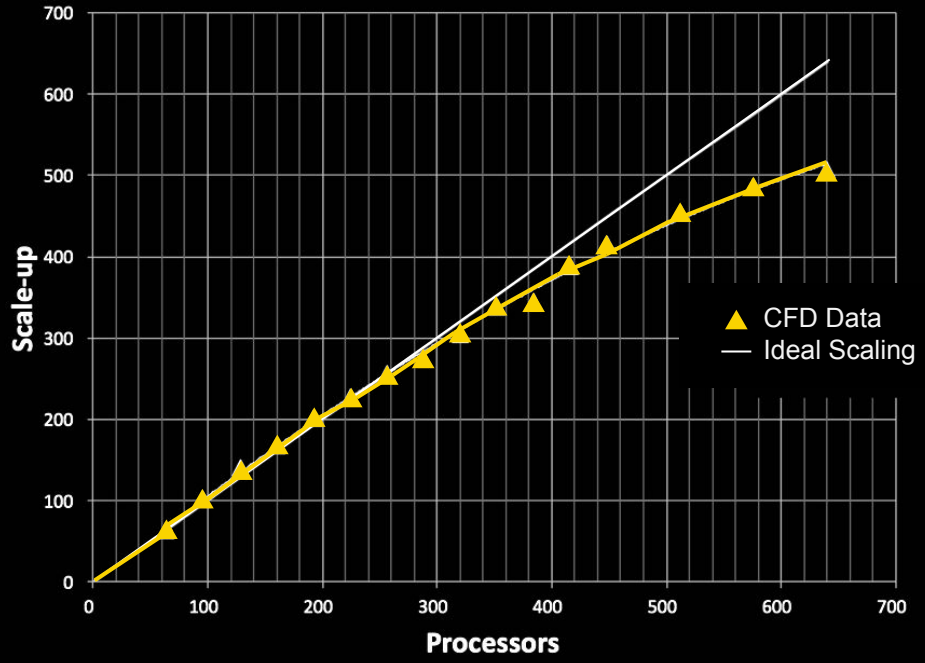
Summit (Oak Ridge National Lab., USA)

- **2,414,592 cores / 148.6 PFLOPS**
- #1 supercomputer (Nov. 2019)

GROUND X Copyright © Ground X. All rights reserved.

figure 1: http://www.hani.co.kr/arti/society/environment/714335.html
figure 2: https://en.wikipedia.org/wiki/Summit_(supercomputer)

Scalable Performance on HPC

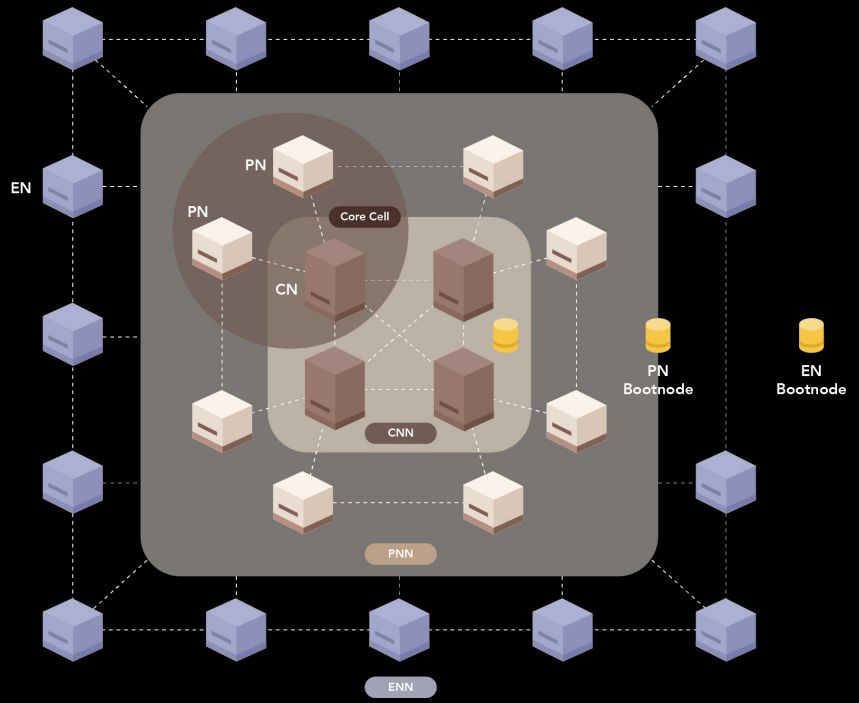


The more the processors (nodes),
The higher the performance

graph: https://aws.amazon.com/blogs/compute/real-world-aws-scalability/

GROUND X Copyright © Ground X. All rights reserved.

How about Current Blockchains?

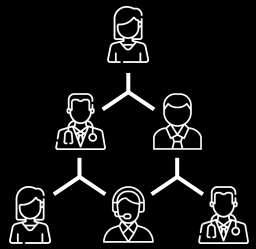


Do They Provide Higher Performance If More Nodes Join the Network?

GROUND X Copyright © Ground X. All rights reserved.

Scalability Trilemma

SECURITY



DECENTRALIZATION

SCALABILITY

No blockchain can have all 3 attributes;
They must choose **2 out of 3** of the attributes.

GROUND X Copyright © Ground X. All rights reserved.

Scaling Solutions

1st Layer (On-Chain)

Sharding (Ethereum)

Hard Fork:

SEGWIT

2nd Layer (Off-Chain)

Service Chain (Klaytn)

Plasma (Ethereum)

Trinity Network (NEO)

Raiden Network (Ethereum)

Lightning Network (Bitcoin)

Distributed Ledgers

Directed Acyclic Graphs:

Tangle:

Block-Lattice:

Consensus Mechanism

Proof-of-Authority:

Byzantine Fault Tolerance
- Delegated:
- Federated:
- Practical:

Delegated Proof-of-Stake:

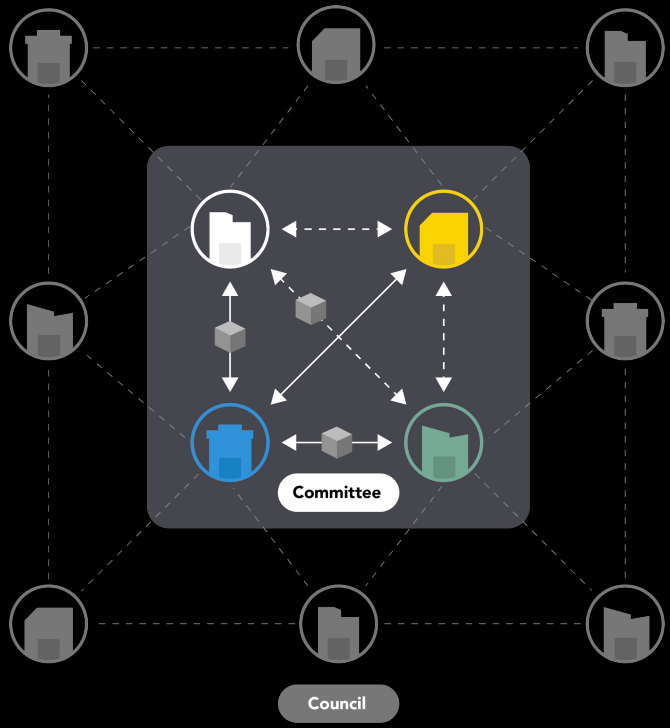
https://masterthecrypto.com/blockchain-scalability-solutions-crypto-scaling-solutions/

GROUND X Copyright © Ground X. All rights reserved.

Klaytn Scalability - Consensus

Securely Scalable BFT

- Trustful node operators form a network called **Governance Council (GC)**
- For each block, Klaytn randomly selects a subset of the council using VRF; we call this subset a **Committee**
- Klaytn runs BFT on a chosen Committee to achieve fast, efficient consensus



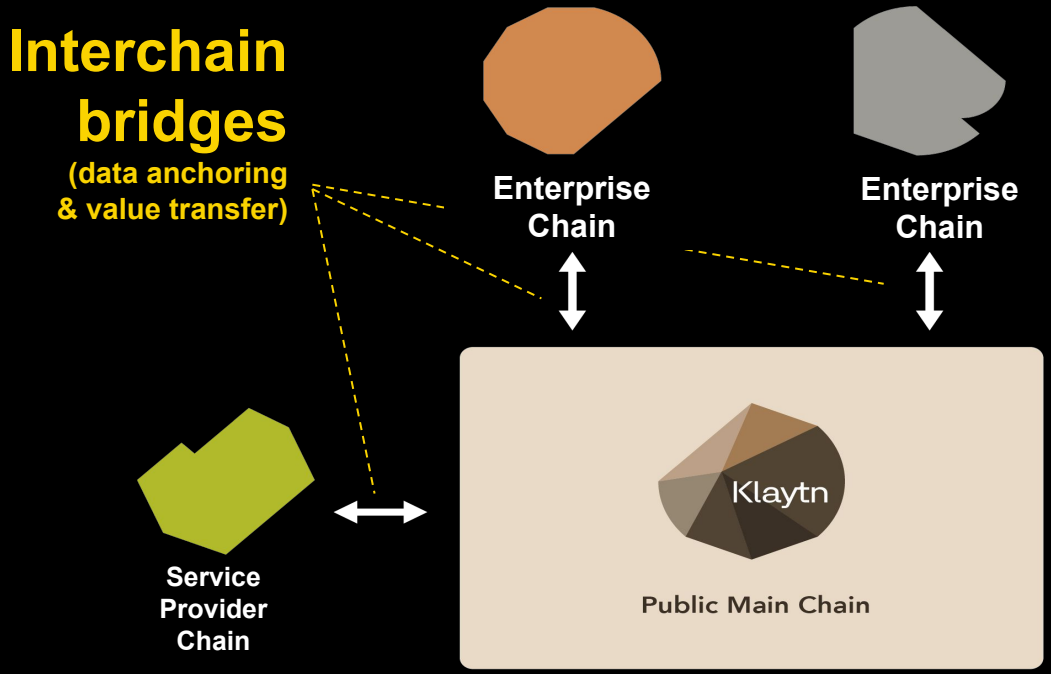
GROUND X Copyright © Ground X. All rights reserved.

Klaytn Scalability - Exploiting Parallelism (1st Layer)

Parallelizing Compute-Intensive Tasks	**Isolating Network Resources**
Limiting Concurrency with a Worker Pool	**Utilizing Fine-Grained Locking**

GROUND X Copyright © Ground X. All rights reserved.

Klaytn Scalability - Service Chain (2nd Layer)

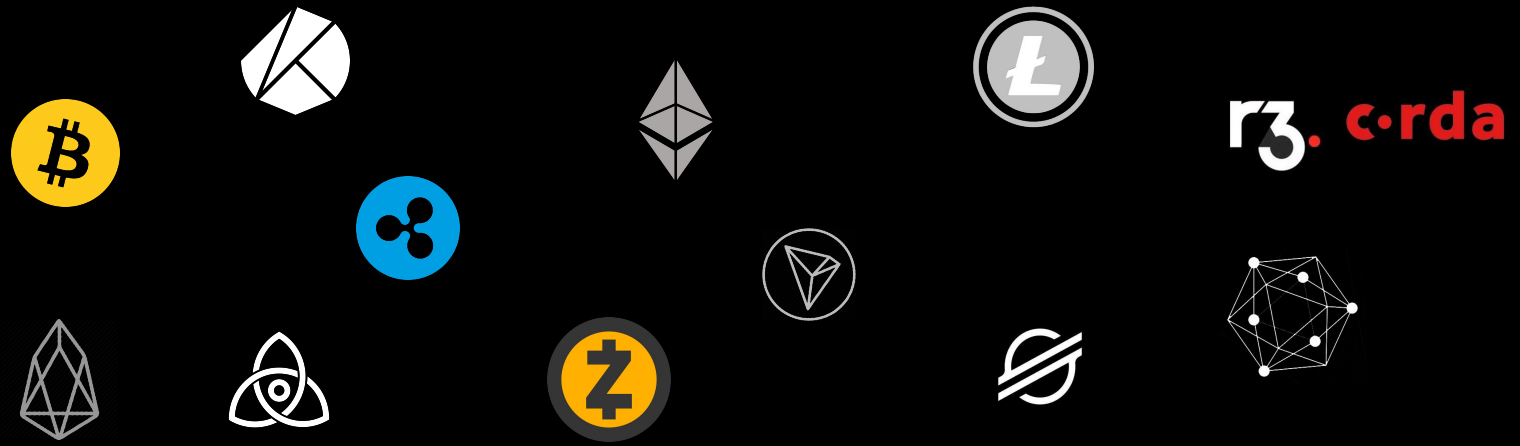


GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge III
Interoperability

GROUND X Copyright © Ground X. All rights reserved.

Can One Blockchain Protocol Rule All Others and Be a Standard?



GROUND X Copyright © Ground X. All rights reserved.

Community says “No”

** Balkanization: becoming a series of unconnected systems operating alongside, but siloed from, each other*

source: https://consensys.net/research/avoiding-blockchain-balkanization/

GROUND X Copyright © Ground X. All rights reserved.

Blockchain Interoperability Methods

Interoperability

- The ability for blockchains to exchange data between platforms
- The ability of any blockchain to be able to prove the state of other blockchains

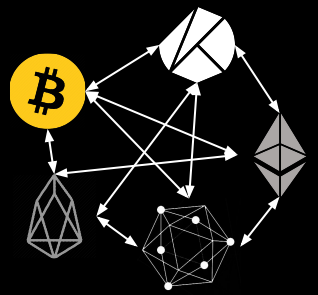
Methods

Notary Schemes

Relaychain & Parachains

Cross-Chain Hash Locking

Multi-Chain Weaving



GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge IV
Security & Privacy

GROUND X Copyright © Ground X. All rights reserved.

Security and Privacy Requirements, Properties and Techniques

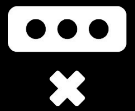
	S&P Requirements	S&P Properties	Corresponding S&P Techniques
Supported in Bitcoin	Consistency	Consistency	Consensus algorithms
	Integrity	Tamper-resistance	Hash chained storage
	Availability	Resistance to DDoS attacks	Consensus algorithms with Byzantine fault
	Prevention of double-spending	Resistance to double-spending attacks	Signature and verification
	Anonymity	Pseudonymity	Public key as pseudonyms
Need to be enhanced	Unlinkability	Unlinkability	Mixing, anonymous signature
	Confidentiality	Confidentiality	ABE, HE, SMPC, NIZK, TEE-based solutions, game-based solutions
		Resistance to the majority (51%) consensus attack	Consensus algorithms that do not depend on computing power

Security and Privacy on Blockchain, Zhang et al., Journal of ACM Computing Surveys, July 2019.

GROUND X Copyright © Ground X. All rights reserved.

Blockchain Security Issues

Key Management



Denial of Service

Endpoint Security

Intentional Misuse

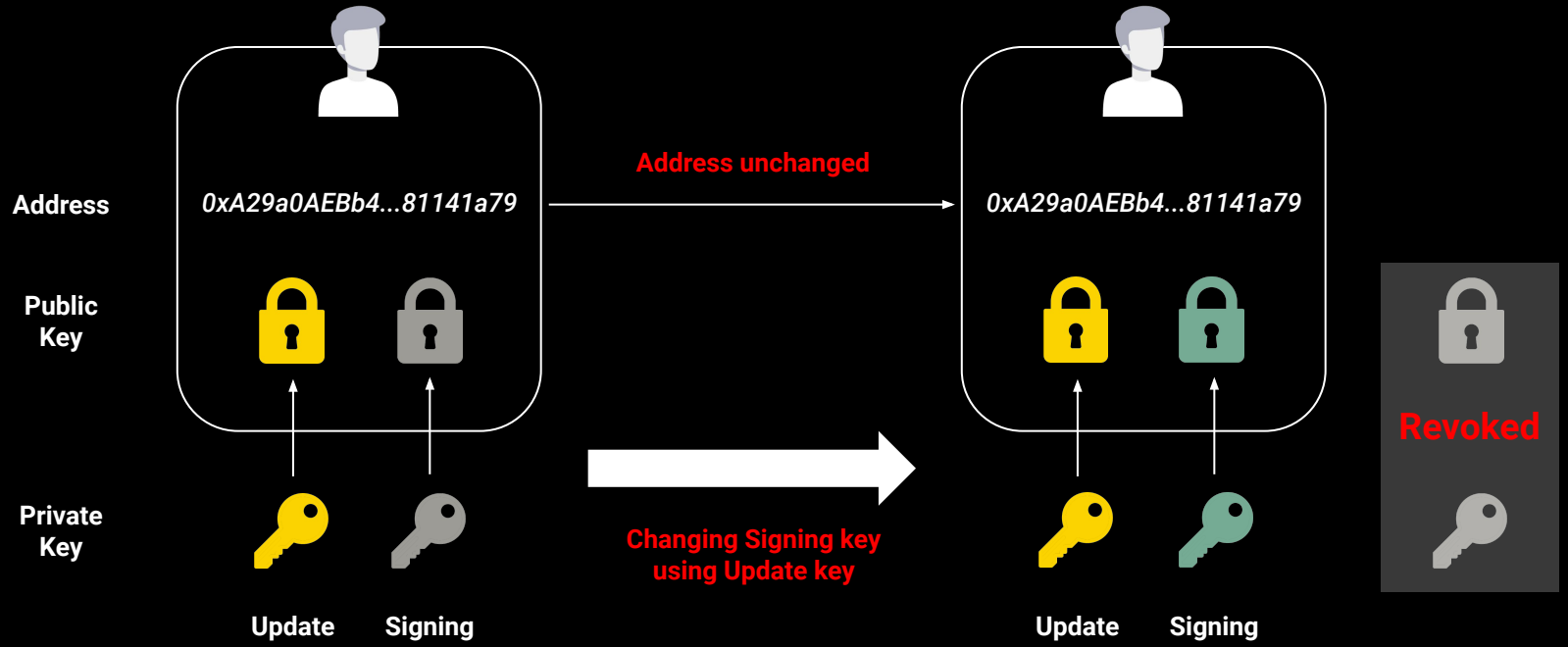
Code Vulnerabilities

Data Protection

GROUND X Copyright © Ground X. All rights reserved.

Klaytn Account Model for Better Security

Improved security with role-based keys: update and signing roles



GROUND X Copyright © Ground X. All rights reserved.

Efforts to Improve Privacy on Blockchain

Privacy Coins

Zero-Knowledge Proof Based

ZCOIN, Bitcoin Private, ZCASH, KOMODO, HORIZEN, PIVX

TOR Based

DeepOnion, VERGE

CoinJoin Based

Dash, CLOAK

Others

MONERO, NAV COIN

Privacy Infrastructure

privatesend, STARKWARE, NUCYPHER, KOVRI, RingCT, zkSNARKs, Bulletproofs, erocoin PROTOCOL

Privacy Decryption

NEUTRINO, CHAINALYSIS, ELLIPTIC

Privacy Layers

COVA COVALENT.AI, KEEP, ORIGO, OASISLABS, enigma

* source: https://konfidio.com/blockchain/explained/what-privacy-coins-are-out-there/

GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge V
Ease of Use and Development

GROUND X Copyright © Ground X. All rights reserved.

Technical Challenge - Ease of Use and Development

User Experience (UX)

Blockchain needs simple, intuitive, and hassle-free UX. Current blockchain UX is similar to the Internet UX before web browsers.

Blockchain Invisibility

Blockchain should be easily used without understanding complicated blockchain technology, just as Internet is used.

Development Environment

Coding, debugging, and testing of blockchain applications should be simpler, and smart contracts should be easily integrated with legacy systems.

Standards

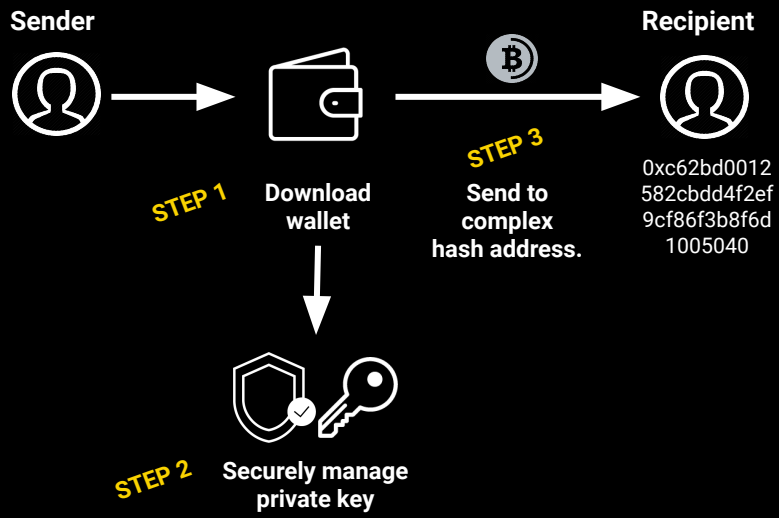
Blockchain needs standards for interoperable interface, migration, and development productivity.

GROUND X Copyright © Ground X. All rights reserved.

Klip's Seamless & Hassle-Free User Experience

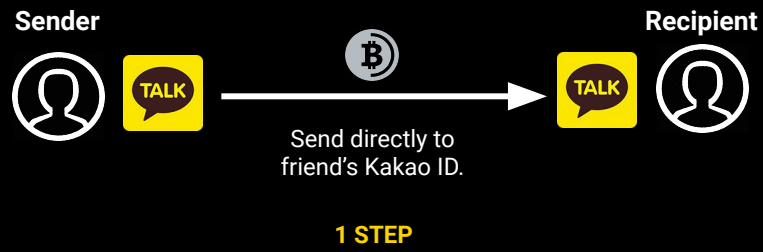
TYPICAL BLOCKCHAIN UX

Typical blockchain user experience is often fragmented



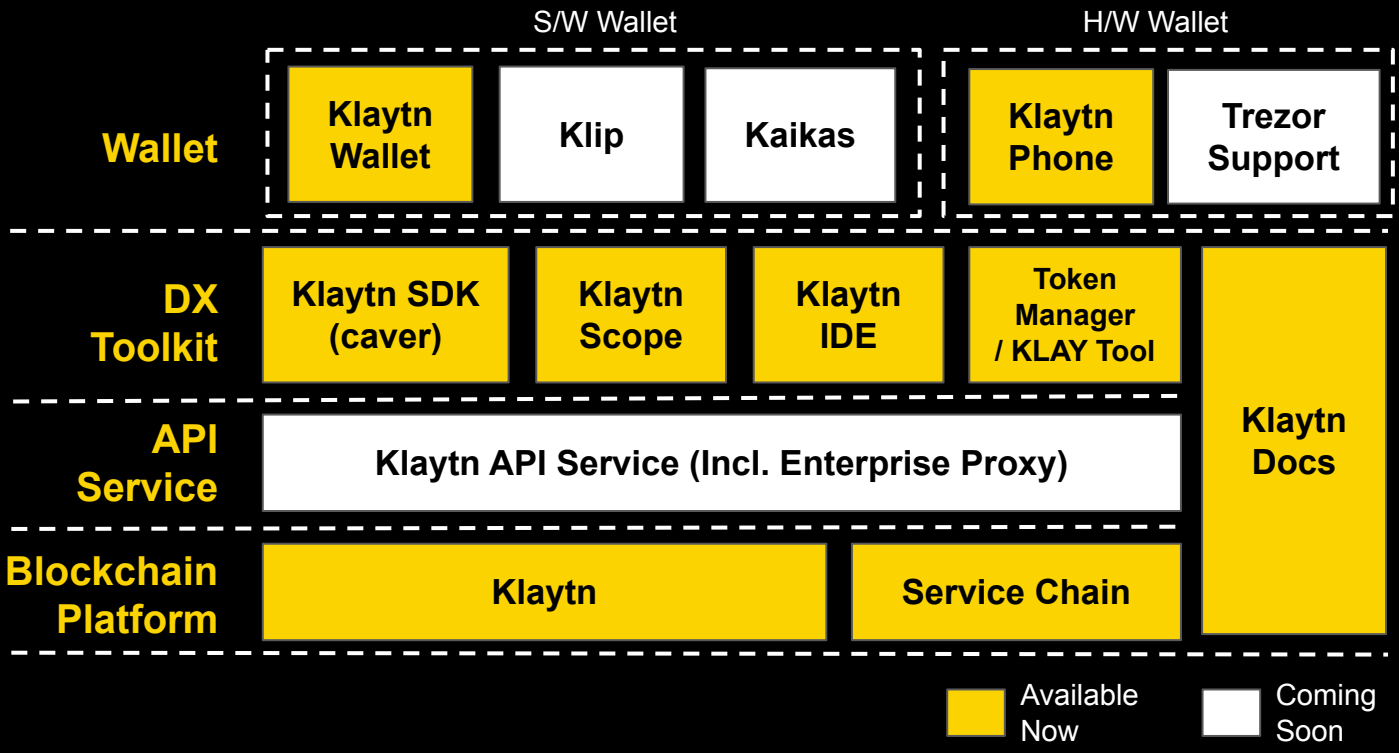
KLIP UX

Integrating with KakaoTalk and Klip offers familiar, seamless user experience



GROUND X Copyright © Ground X. All rights reserved.

Klaytn Developer Tools

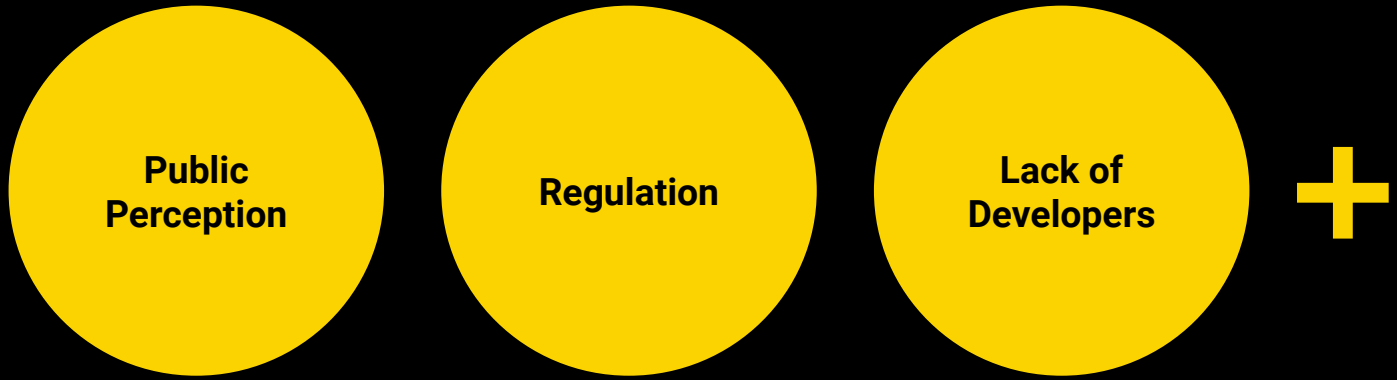


GROUND X Copyright © Ground X. All rights reserved.

Non-Technical Challenges

GROUND X Copyright © Ground X. All rights reserved.

Non-Technical Challenges



GROUND X Copyright © Ground X. All rights reserved.

Non-Technical Challenge I
Public Perception

GROUND X Copyright © Ground X. All rights reserved.

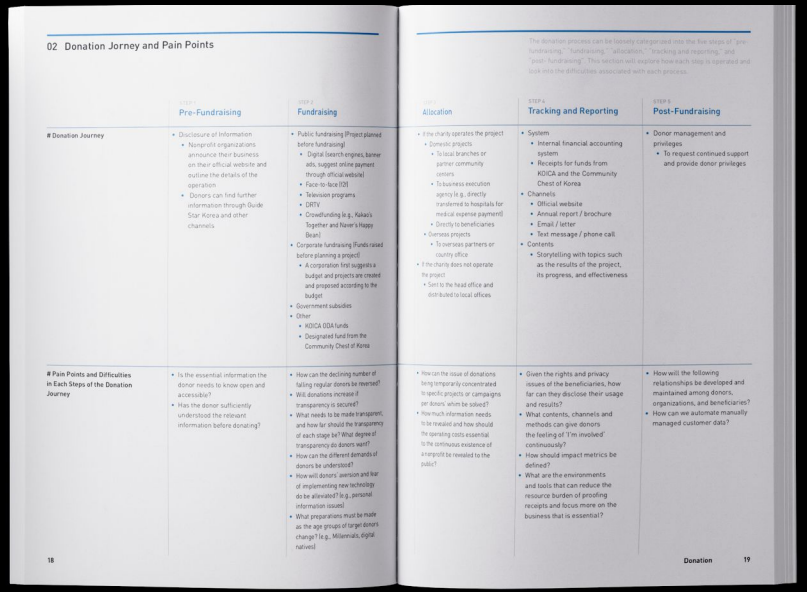
Public Perception on Blockchain

- Challenge of anonymity
  - Money laundering
- Criminal connection
  - Bitcoin used in the black market and the dark web
- Needs public acknowledgement and marketing

fig: https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#2616d8eb3bdc

GROUND X Copyright © Ground X. All rights reserved.

Ground X's Leadership on Blockchain for Social Impact



GROUND X Copyright © Ground X. All rights reserved.

Non-Technical Challenge II
Regulation

GROUND X Copyright © Ground X. All rights reserved.

Regulation on Blockchain

- Lack of regulation
  - Users fear losing their investments and are less motivated to adopt blockchains
- “Regulation is the first key for establishing blockchain technology at it will provide the lacking level of trust.”
  - Julian-Andre Winter, head of asset management at The Naga Group

GROUND X Copyright © Ground X. All rights reserved.

Blockchain Regulation in Progress

coingeek NEWS CONFERENCES HOW TO BUY BSV? VENTURES

TECH 3 NOVEMBER 2019 Steve Kaaru

This week in tech: Blockchain regulation takes center stage in China, Korea, India and more

Blockchain technology is going to power the future—that much is clear. But in order to do so, there must be enabling regulations and policies that can foster its growth. More countries are recognizing this, and this week saw quite some effort to
number of global powerhouses. China continued in its r
crypto and blockchain hub, with India, Korea and even A
week also saw a number of blockchain startups raise fur
founder invested in.

More than just crypto: blockchain usage grows amidst greater regulation

By Emma Olsson | 19 November 2019

With countries such as China and Germany laying the groundwork for their blockchain legislation in the past few months, and financial services still undecided on the uses of blockchain, it is apt to re-evaluate the uses of the distributed ledger technology (DLT).

Blockchain often connotes cryptocurrencies, but the technology has many uses: increasing speed and security in cross-border transactions, smart contracts, digital identity – to name a few. As blockchain regulation becomes more commonplace, the application of the technology has the potential to grow in prevalence.

Chinese Government Forms New Committee to Regulate Blockchain Technology

By ALLISON JIANG 3 days ago

Home > Daily Drip > Chinese Government Forms New Committee to Regulate Blockchain Technology

In a highly centralized country like China, blockchain technology has always been slightly rocky terrain. But China's ever-evolving relationship with blockchain took a new step forward on Wednesday when the Standardization Administration of China (SAC) announced the formation of a national standards committee for blockchain regulation.

The SAC, which is authorized by the Chinese government and represents China in the International Organization for Standardization, released a statement that the organization is assembling several technological committees to improve China's "economic development and social governance." This included blockchain and other elements of the sharing economy.

NEWS

Nov 25, 2019

News Op-Eds Press Releases About Advertise Publish Press Release The Satoshi Re

REGULATION
by Kevin Helms
Oct 31, 2019

Korean Presidential Committee Pushes to Legalize Crypto

GROUND X Copyright © Ground X. All rights reserved.

Non-Technical Challenge III
Lack of Developers

GROUND X Copyright © Ground X. All rights reserved.

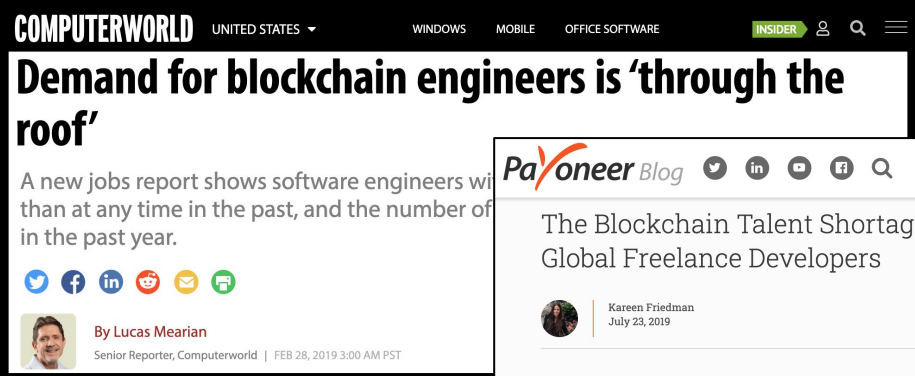
Lack of Developers

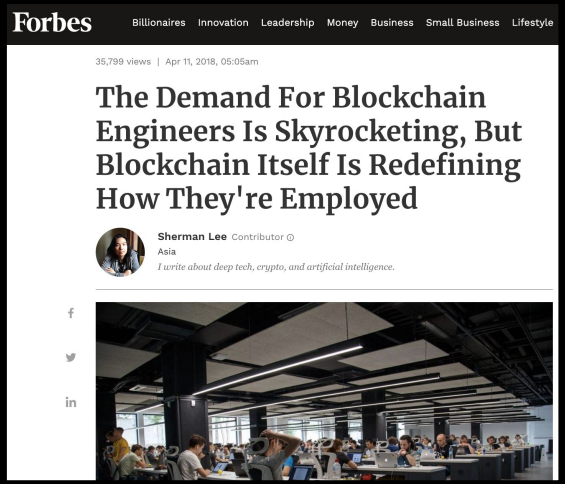
Lack of Skilled Developers

Finding capable software engineers for developing blockchains or apps is too tricky.

Lack of Education

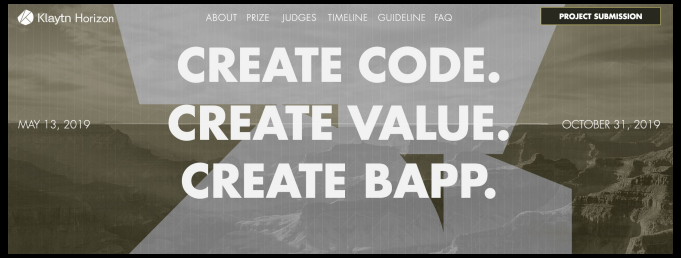
One barrier hindering blockchain technology diffusion is the lack of proper education on the innovative technology.

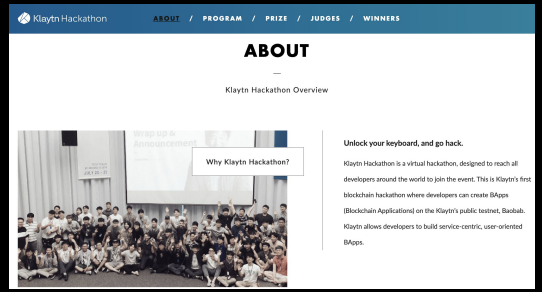


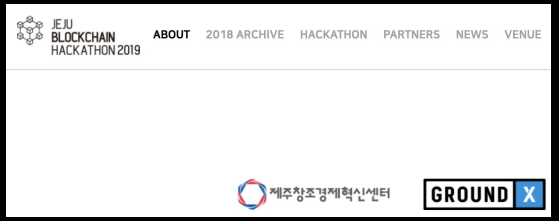


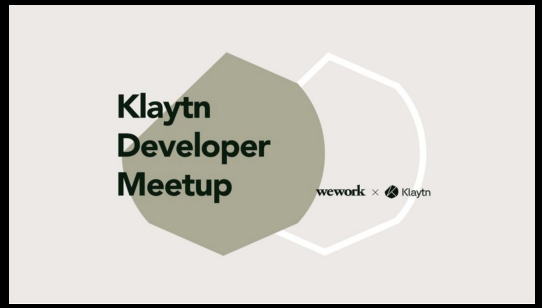
GROUND X Copyright © Ground X. All rights reserved.

Klaytn's Community Activities



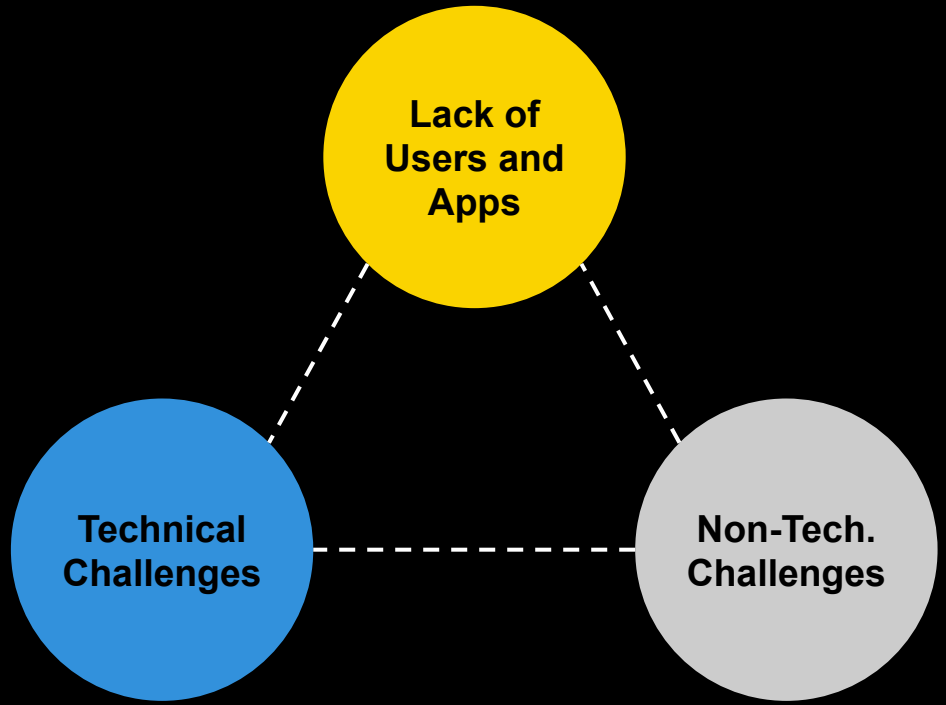






GROUND X Copyright © Ground X. All rights reserved.

Challenges for Blockchain Mass Adoption



- Performance
- Scalability
- Interoperability
- Security & Privacy
- Ease of Use & Development
- ...

- Public Perception
- Regulation
- Lack of Developers
- ...

GROUND X Copyright © Ground X. All rights reserved.

It’s Time to Build.

GROUND X Copyright © Ground X. All rights reserved.

THANK YOU

Ground X
27F, 521, Teheran-ro,
Gangnam-gu, Seoul, Republic of Korea

GROUND X Copyright © Ground X. All rights reserved.