Challenges for Blockchain Mass Adoption
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
Are We Using Blockchains in Everyday Life?
Blockchain Mass Adoption?

We are here

Hype Cycle and Technology Adoption Lifecycle Plotted together

Challenges for Blockchain Mass Adoption
Challenges for Blockchain Mass Adoption

- Lack of Users and Apps
- Technical Challenges
  - Performance
  - Scalability
  - Interoperability
  - Security & Privacy
  - Ease of Use & Development
  - ...
- Non-Tech. Challenges
  - Public Perception
  - Regulation
  - Lack of Developers
  - ...

Copyright © Ground X. All rights reserved.
Lack of Users and Apps
## The State of Apps and Platforms

<table>
<thead>
<tr>
<th></th>
<th>Mobile Apps</th>
<th>Blockchain Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of APPS</td>
<td>~5.8 M</td>
<td>~2,000</td>
</tr>
<tr>
<td>Number of Users</td>
<td>~250 M</td>
<td>~2.4 M</td>
</tr>
<tr>
<td>Key Players</td>
<td><img src="https://via.placeholder.com/150" alt="Google" />, <img src="https://via.placeholder.com/150" alt="Facebook" />, <img src="https://via.placeholder.com/150" alt="Amazon" /></td>
<td><img src="https://via.placeholder.com/150" alt="Ethereum" />, <img src="https://via.placeholder.com/150" alt="Tron" />, <img src="https://via.placeholder.com/150" alt="EOS" /></td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Platform</th>
<th>Total DApps</th>
<th>Daily active users</th>
<th>Transactions (24hr)</th>
<th>Volume (24hr)</th>
<th># of contracts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethereum</td>
<td>2,690</td>
<td>23.04k</td>
<td>83.37k</td>
<td>189.98k</td>
<td>3.9k</td>
</tr>
<tr>
<td>EOS</td>
<td>313</td>
<td>11.44k</td>
<td>420.41k</td>
<td>334.39k</td>
<td>480</td>
</tr>
<tr>
<td>Steem</td>
<td>91</td>
<td>9.26k</td>
<td>325.65k</td>
<td>105.83k</td>
<td>160</td>
</tr>
<tr>
<td><strong>Klaytn</strong></td>
<td><strong>21</strong></td>
<td><strong>40.55k</strong></td>
<td><strong>204.32k</strong></td>
<td><strong>0</strong></td>
<td><strong>53</strong></td>
</tr>
<tr>
<td>POA</td>
<td>19</td>
<td>208</td>
<td>3.55k</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>NEO</td>
<td>17</td>
<td>1.85k</td>
<td>5.33k</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>xDai</td>
<td>12</td>
<td>5</td>
<td>7</td>
<td>0</td>
<td>39</td>
</tr>
<tr>
<td>Loom</td>
<td>10</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>70</td>
</tr>
<tr>
<td>GoChain</td>
<td>7</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>17</td>
</tr>
<tr>
<td>OST</td>
<td>2</td>
<td>54</td>
<td>694</td>
<td>17.31k</td>
<td>2</td>
</tr>
</tbody>
</table>

* Data collected on Nov. 25, 2019
Since its launch in June 2019, Klaytn Mainnet successfully established rapid rate of adoption and growth by business entities.
Technical Challenges
Technical Challenges

- Performance
- Scalability
- Interoperability
- Security & Privacy
- Ease of Use & Development
Technical Challenge I

Performance
### Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment

Logistics, Litke et. al. (2019).

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Ethereum</th>
<th>Ripple</th>
<th>EOS</th>
<th>Stellar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to finality</td>
<td>15 min</td>
<td>6 min</td>
<td>4 sec</td>
<td>180 sec</td>
<td>2-5 sec</td>
</tr>
<tr>
<td>Transactions per second (TPS)</td>
<td>7</td>
<td>15</td>
<td>1,500</td>
<td>3,000</td>
<td>1,000</td>
</tr>
</tbody>
</table>
Klaytn Cypress Performance

Latency

1 sec
block interval

Enables mobile app-like performance

Throughput

4,000 TPS

Supports production-grade enterprise usage
Technical Challenge II

Scalability
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)

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/
How about Current Blockchains?

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

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

1st Layer (On-Chain)

- Shard (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

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
Klaytn Scalability - Exploiting Parallelism (1st Layer)

- Parallelizing Compute-Intensive Tasks
- Isolating Network Resources
- Limiting Concurrency with a Worker Pool
- Utilizing Fine-Grained Locking
Klaytn Scalability - Service Chain (2nd Layer)

Interchain bridges
(data anchoring & value transfer)

Enterprise Chain

Enterprise Chain

Service Provider Chain

Public Main Chain

Klaytn
Technical Challenge III

Interoperability
Can One Blockchain Protocol Rule All Others and Be a Standard?
Community says “No”

Avoiding Blockchain Balkanization

Lessons from the early Internet on why we need blockchain interoperability

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

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

Security & Privacy
## Security and Privacy Requirements, Properties and Techniques

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

Blockchain Security Issues

Key Management  Denial of Service  Endpoint Security

Intentional Misuse  Code Vulnerabilities  Data Protection
Klaytn Account Model for Better Security

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

- Address: 0xA29a0AEBb4...81141a79
  - Public Key: Update and Signing
  - Private Key: Update (Revoked)

- Address unchanged: 0xA29a0AEBb4...81141a79
  - Public Key: Update and Signing
  - Private Key: Signing

---

Copyright © Ground X. All rights reserved.
## Efforts to Improve Privacy on Blockchain

### Privacy Coins

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-Knowledge Proof Based</td>
<td>Zcoin, Bitcoin Private</td>
</tr>
<tr>
<td></td>
<td>Zcash, Komodo, Horizen PIVX</td>
</tr>
<tr>
<td>TOR Based</td>
<td>DeepOnion, Verge</td>
</tr>
<tr>
<td>CoinJoin Based</td>
<td>Dash, Cloak</td>
</tr>
<tr>
<td>Others</td>
<td>Monero, NAV, NUCYpher</td>
</tr>
</tbody>
</table>

### Privacy Infrastructure

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>privatesend</td>
</tr>
<tr>
<td>Starkware</td>
</tr>
<tr>
<td>Nucypher</td>
</tr>
<tr>
<td>Kovri</td>
</tr>
<tr>
<td>zkSNARKs</td>
</tr>
<tr>
<td>Bulletproofs</td>
</tr>
<tr>
<td>Ercocin</td>
</tr>
</tbody>
</table>

### Privacy Decryption

<table>
<thead>
<tr>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutrino</td>
</tr>
<tr>
<td>Chainalysis</td>
</tr>
<tr>
<td>Elliptic</td>
</tr>
</tbody>
</table>

### Privacy Layers

<table>
<thead>
<tr>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covalent.ai</td>
</tr>
<tr>
<td>Keep</td>
</tr>
<tr>
<td>Enigma</td>
</tr>
<tr>
<td>Oasis Labs</td>
</tr>
</tbody>
</table>

* source: https://konfidio.com/blockchain/explained/what-privacy-coins-are-out-there/
Technical Challenge V
Ease of Use and Development
## Technical Challenge - Ease of Use and Development

<table>
<thead>
<tr>
<th>User Experience (UX)</th>
<th>Blockchain Invisibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain needs simple, intuitive, and hassle-free UX. Current blockchain UX is similar to the Internet UX before web browsers.</td>
<td>Blockchain should be easily used without understanding complicated blockchain technology, just as Internet is used.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Development Environment</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding, debugging, and testing of blockchain applications should be simpler, and smart contracts should be easily integrated with legacy systems.</td>
<td>Blockchain needs standards for interoperable interface, migration, and development productivity.</td>
</tr>
</tbody>
</table>
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

**Sender** → **Recipient**

**STEP 1**
Download wallet

**STEP 2**
Securely manage private key

**STEP 3**
Send to complex hash address.

Example hash address:
0xc62bd012582cbddd4f2ef9cf86f5b8f6d1005040

**Sender** → **Recipient**

**1 STEP**
Send directly to friend’s Kakao ID.
Klaytn Developer Tools

- **Wallet**
  - S/W Wallet
    - Klaytn Wallet
    - Klip
    - Kaikas
  - H/W Wallet
    - Klaytn Phone
    - Trezor Support

- **DX Toolkit**
  - Klaytn SDK (caver)
  - Klaytn Scope
  - Klaytn IDE

- **API Service**
  - Klaytn API Service (Incl. Enterprise Proxy)
  - Token Manager / KLAY Tool

- **Blockchain Platform**
  - Klaytn
  - Service Chain

**Available Now**

**Coming Soon**
Non-Technical Challenges
Non-Technical Challenges

- Public Perception
- Regulation
- Lack of Developers
Non-Technical Challenge I
Public Perception
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
Ground X’s Leadership on Blockchain for Social Impact
Non-Technical Challenge II

Regulation
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
Blockchain Regulation in Progress

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 that end. A number of global powerhouses. China continued in its role as a crypto and blockchain hub, with India, Korea and even Australia also looking into blockchain. The week also saw a number of blockchain startups raise funds, with a number of founders invested in.

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.

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.
Non-Technical Challenge III

Lack of Developers
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.
Klaytn’s Community Activities
Challenges for Blockchain Mass Adoption

- Lack of Users and Apps
  - Technical Challenges
    - Performance
    - Scalability
    - Interoperability
    - Security & Privacy
    - Ease of Use & Development
    - ...
  - Non-Tech. Challenges
    - Public Perception
    - Regulation
    - Lack of Developers
    - ...

- ...
It’s Time to Build.
THANK YOU