BGIN BMR_9

BGIN Block #9 Meeting Report

- Rebuilding Value, Governance and Reputation on Blockchain -

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

The know-how described in this document was made available from contributions from various sources, including members of the BGIN and others. Although the BGIN has taken steps to help ensure that the know how is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the know how described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. BGIN and the contributors to this document make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

Table of contents

1. Meeting Overview

1.1. Meeting Dates/Venue

- Dates: Sunday, Nov. 19, 2023, to Wednesday, Nov. 22, 2023
- Venue: Collider at 477 on Pitt Street (Day 1,4) / Sydney Startup Hub (Day2, 3)
  Sydney, Australia

1.2. Participants

- In-person registrations: 74
- Online-registrations: 54

1.3. Event Sponsors

- Special
  - NTT Digital
- Level 1 Sponsors
  - Casper Network
- Level 2 Sponsors
  - Circle
  - Digital Garage
  - LIGHTLINK
  - MUFG Bank
  - Nomura Research Institute
  - RECRUIT

1.4. Meeting Web Page

https://bgin-global.org/events/20231119-block9

2. Timetable

Please visit the following link for the details
https://bgin-global.org/events/20231119-block9

3. Session Summary

3.1. Opening Plenary

Date: Nov. 19, 2023
Time: 14:15 - 14:45
Speaker: Chloe White (Genesis Block, DTWG Co-Chair)
Video: https://www.youtube.com/watch?v=dhfDvm_Z4Dg&t=1319s
Summary:
-

3.2. Round Table 1: Reconsidering Blockchain Governance

Date: Nov. 19, 2023
Time: 14:45 - 15:30
Speakers:

- Joseph Beverly (Soulbis, Local Chair)
- Ryosuke Ushida (JFSA)
- Katya Delak (NIST)
- Amanda Wick (Association for Women in Cryptocurrency)
- Dr. Mark Staples (DFCRC)
- Gerard Dache (Government Blockchain Association)

Video: https://www.youtube.com/watch?v=DkrnEGJ9ycI
Summary:

- Questions that were discussed
    - How should regulatory frameworks adapt to the pace of blockchain innovation without stifling it?
    - In what ways can international standards be developed to ensure interoperability in blockchain systems, while respecting the sovereignty of nations?
    - What measures can be instituted to ensure that blockchain governance structures are inclusive and represent a diverse set of stakeholders?
    - Considering the inherent risks associated with blockchain technologies, how can governance models be structured to protect consumers and maintain systemic stability?
    - How can collaboration between the public and private sectors be optimised to foster both innovation and public trust in blockchain systems?
    - With increasing scrutiny on the environmental impact of technology, what role does governance have in ensuring the sustainability of blockchain operations?
    - What are the key considerations for designing a blockchain governance framework that is resilient and adaptable to future technological advancements?

3.3. Round Table 2: Best Practice for Blockchain Governance

Date: Nov 19, 2023

Time: 15:45 - 16:30
Speakers:

- Mitchell Travers (Soulbis, IKP WG Co-Chair)
- Amanda Wick (Association for Women in Cryptocurrency)
- Dr. Mark Staples (DFCRC)

Video: https://www.youtube.com/watch?v=3t4BBurHO8k&t=1s
Summary:

- Questions that were discussed
    - What is the current state of global standardisation in blockchain governance, and how can uniform standards be agreed upon and applied?
    - How can ethical considerations be integrated into blockchain governance frameworks to ensure equitable outcomes?
    - What strategies are effective in engaging a broad range of stakeholders in the governance process, particularly those traditionally underrepresented?
    - How can governance frameworks be designed to be both compliant with current regulations and adaptable to future legislative changes?
    - What are the main challenges in creating governance structures that are effective across different jurisdictions, and how might these be overcome?
    - Which emerging trends in blockchain technology present the most significant governance challenges and opportunities?
    - What metrics or indicators are most useful in assessing the effectiveness of a blockchain governance model?

3.4. Round Table 3: Decentralized vs Centralized Primary Issuance: Governance and Security Challenges

Date: Nov 20, 2023
Time: 9:45 - 10:30
Speaker:

- Chloe White (Genesis Block, DT WG Co-Chair)
- Michaela Juric (Novatti, AUDD)
- Will Remor (MakerDAO)
- Dr. Mark Staples (DFCRC)

Video: https://www.youtube.com/watch?v=4cA2oJlnNFg
Summary:

- Tokenization is an inherently centralized act, and there is always a single point of failure. Public blockchains only have the property of transferring ownership of ‘digital things’, but they become centralized because the representation of assets becomes tangible through human action.
- When considering security in terms of confidentiality, integrity, and availability, one of the characteristics of blockchain integrity is that once deployed, the code is difficult to change, but for token integrity, not only the integrity of the information and the tokenization process but also the integrity of the token backing is important.
- Novatti, which issues AUDDs, has adopted a multi-signature scheme that requires consensus for the issuance of AUDDs as a security risk measure related to the issuance. Issuance is determined by a vote using a governor's token by a person called a distributor.

3.5. Round Table 4: The Harmonisation of CBDC, Deposit Token, Stablecoin, Crypto Assets and DeFi

Date: Nov 20, 2023
Time: 10:30 - 11:15
Speaker:

- Stephanie Bazley (Possible Ventures)
- James Angel (Georgetown University)
- Masaki Bessho (Bank of Japan)
- Paul Travers (KPMG Risk and Treasury)
- Alejandro Galluci (DeFactor)
- Andrew Galluci (Circle)
- Hiromi Yamaoka (DeCurrent DCP)

Video: https://www.youtube.com/watch?v=cJMuBRhtUAc
Summary:

- The central bank will focus on ensuring the unity of money (i.e., that money, regardless of its nature, has the same value and the same power). To ensure the same convertibility as central bank-issued money, private money such as stablecoin requires regulatory arrangements that complicate banking and consumer protection, segregation of customer assets, etc.

3.6. Round Table 5: Digital Asset Standardization and R&D Strategy

Date: Nov 20, 2023
Time: 11:30 - 12::15
Speaker:

- Carole House (ex-White House)
- Craig Dunn (TC307 Chair)
- Katya Delak (NIST)
- Julien Bringer (Kallistech)
- Dr. Mark Staples (DFCRC)

Video: https://www.youtube.com/watch?v=yCUPv9xUTLA&t=2s
Summary:

- While there are many technical standards related to digital assets in different technical fields and at different levels of detail and abstraction, most of the standards in ISO Technical Committee TC307 are intended to increase conceptual understanding in the industry and to improve productivity across organizations and companies.
- It is neither too early nor too late to introduce standards for emerging technologies. If too early, inefficient technologies will be reinforced, while chaos will ensue if too late. It is not a simple matter and we need decision-making through consensus.
- Standardization organizations must be able to attract people who are interested in developing standards, have expertise, and are willing to devote time to it. Since most startups do not have the time to devote, it is often the larger companies that have the resources to commit to the development of standards.

- While the core developers of Bitcoin state that the protocol itself is the standard, there is a standardization process for all other protocols. at Cosmos, there were once efforts to develop a governance standard for validators. However, the effort itself was stalled due to various concerns and pressures regarding the legal responsibilities of validators, as well as contractual obligations to investors, etc., that would have dictated the actions of validators.

3.7. DTWG Interactive Workshop Session 1: Points of Failure of Stablecoins

Date: Nov 20, 2023
Time: 13:30 - 15:00
Session Chair: Chloe White (Genesis Block, DTWG Co-Chair)
Summary:

- The Price Stability Module (PSM) was initially a way for bringing liquidity for illiquid stablecoins in the marketplace. The PSM was created because of too much demand for DAI and DAI was constantly off-peg. The PSM has been created as a way for DAI to trade on a 1-1 basis without no arbitrage, arbitrage being made on secondary markets.
- When COVID hit, the Maker protocol generated some bad debt in the system, and therefore had to liquidate some of the governance assets to offset the debt. The liquidation of the auctioning wasn't working properly in terms of creating an efficient auction system, leading to a whole six months of developing Liquidation 2.0. The crisis has created something new and the community moves forward. The next potential area to be improved might be friction on redemption, which can be another research topic.
- MakerDAO is evolving toward a so-called sub-DAO framework. now moving towards essentially the original version of the Maker project, reducing the amount of governance at the core of the Maker protocol to try to look like Bitcoin and be autonomous without human interaction and delegating functions toward other DAOs. Such mini-DAOs are functionally specific to deal with different problems. From a risk perspective, one of the key things for consideration is whether DAI will have the liquidity transmission mechanism from the core into the min-DAOs. The very first experiment of the liquidity transmission now we are seeing is called the Spark protocol, which was officially launched a couple of months ago.
- In terms of applying capital requirements to DeFi, MakerDAO actually started it 3 or 4 years ago. They start collating some information on how tier 1 capital will actually work, additional tier 1 capital, risk-weighted assets, etc. Sometimes applying exactly the same standards for them is a challenge. They had to be slightly adapted to the situation in which Maker was placed, but now it could change because of a hierarchical acceptance of a lot less volatile asset like ETH.
- When it comes to delegation, the question is how people actually use frameworks and how they delegate. Are there any communities and councils of people who can provide value to things that help actually communities put forward?
- In terms of conflicts of interest among DAO participants, you can find beneficiary ownerships and entities without necessarily disclosing them. If you have privacy assets, they need to be protected but we need to discuss what kind of disclosures actually need to exist in this space.

3.8. DTWG Interactive Workshop Session 2: Transparency of DApps and Sound DeFi

Date: Nov 20, 2023
Time: 13:30 - 15:00
Session Chair: Joseph Beverley (Soulbis, Local Chair)
Summary:

- There is research that analyzes different DeFi protocols, finding that there are centralized elements in them. Some of them could fall into the definition of centralized entity in existing regulations and might be able to apply the same ones to them. Discussion on what requirements we should regulate and what we should not is a great start.
    - Considering who should be regulated, it comes down to the fundamental question of what are DeFi protocols. Is it seen as just a bunch of code that runs itself, or is it a different kind of exchange that is developed by a small group of responsible engineers?
    - Regulators should not regulate software or protocol itself but can identify entities that are responsible for them and regulate them. To identify them, regulators need to look at various kinds of potentially responsible entities.
    - We have never seen a case of anyone who has created a DeFi protocol that has been railroaded and then walked away. They don't walk away after all, they decide on the stations and when the trains will run in order to make money on the backend. (On the other hand, one could argue that although centralized, they are in a position of control by multiple entities rather than 100% centralization and are moving toward long-term decentralization.)
    - If custodial service providers are subject to the rigorous regulatory regime, it means we can control the access layer then we may be able to achieve some regulatory outcomes without regulating protocols themselves.

- Privacy Pool Discussion
    - We are on a (blockchain) system where law enforcement and regulatory authorities want to know ‘who’ if there is something suspicious, and many of the protocols do not incorporate anything effective that helps law enforcement and authorities judge things. Each protocol should begin by explaining what preventative measures are in place to ensure that they are preventing ML/FT. Starting with basic standards would give the industry a great deal of credibility.
    - Even though it is public and open, blockchain data is transaction-based, and when it comes to identifying who it is, in fact, even Chainanalysis can only map less than 50%. Even though all the data on the blockchain is open and transparent, it is not personally identifiable information.

3.9. DTWG Interactive Workshop Session 3: CBDC and Privacy

Date: Nov 20, 2023
Time: 15:30 - 17:00
Session Chair: Joseph Beverley (Soulbis, Local Chair)
Summary:

- You can’t achieve privacy through anonymity. Privacy and anonymity are not the same thing. Privacy means that there is data that is discoverable and disclosable under certain conditions, permissions, and protections. The idea of governments enabling complete anonymity across CBDC activities is a non-starter.
- What are the ways to put privacy controls around activities with CBDC? Is there a way that governments should be okay with allowing any type of transaction with no discoverability? The answers are unique based on the jurisdictional context.
- As an investigator, gaining access to financial data that the government possesses is very difficult. Simply because the government possesses data it does not mean they can access it. But governments also legislate what the thresholds are and how they are applied, and perhaps what the criteria are is not always clear. There should be a discussion around data access vs possession.
- The concept of privacy has evolved over time. It has since evolved to the right of control over personal information. But in academic areas, the concept of privacy has evolved even further and some academics argue that the right of privacy is the right to control your personality. How should you mitigate the risks of profiling is becoming a key topic. In the context of CBDC, the confidentiality of the legal entity data would need to be considered, as the limitation of privacy is that it only applies to natural persons.
- If central banks were to introduce CBDC, A desirable feature might be a cash-like one. The central bank does not have any motivation to possess personal data. Having or accessing personal data might do harm to their credibility. Besides, concerns about privacy might have a bad influence on the adoption of CBDC. If looking at the positive aspects of privacy-preserving features, it might mitigate the risks of data enclosure by BigTech and empower customers’ bargaining power on their personal data. However, the privacy feature of CBDC cannot be limitless. The failure to comply with AML/CFT could significantly harm the confidence of a CBDC system itself. Another issue is the necessity of a measure to mitigate the impact to the financial system.
- One of the beautiful things about CBDCs rather than smart contracts is that you can encode them. You can encode the rules of a CBDC in such a way that complies with legislation so that you can actually test out and see, do we like this or do we not like this? Is this enough privacy or not? This type of technical study has not been conducted yet.
- Fitting code to legislation or changing legislation to fit the use case?: design should come first and legislations should follow. We shouldn’t excessively persist to the existing legal regimes, and instead we should think over the optimal design of CBDC first and consider how we could fit the design to the legal arrangements.
- If you cant get legislative support to enace a framework that allows it, the beauty of perfect stablecoin with perfect levels of privacy with perfect operators does not matter because you can’t get people to mobilize in a democratic environment. We have to go to the level of how we sell it.

- In many jurisdictions trust over the commercial banks are quite high. Most central banks are aiming to introduce CBDC in a 2-tier distribution model wheere the commercial banks or other intermediaries expect to work as intermediaries for CBDC and the data that can identify specific person should be exclusively stored within commercial banks and for exceptional occasions at central bank. In these models, the governments have no access to such personal identifiable data.

3.10. DTWG Interactive Workshop Session 4: Smart Contract Security, Governance, and Impact of AI

Date: Nov 20, 2023
Time: 15:30 - 17:00
Session Chair: Ellie Rennie (RMIT)
Summary:

- Smart contract engineers were very thin on the ground several years ago, but codified taxonomies have arisen as a part of their emerging professionalism. It has got a baseline, a useful set of inputs for AI, in a programmatic sense.
- Can we use blockchain technology to help with the governance of AI models? Is there a way for these AI models to upload on-chain attestation? If one day OpenAI gives you a model that is widely open source, billions of numbers of data will be in a CSV file, which is hard to read even if you have access.
- In terms of using AI to read smart contract data, smart contract data today in EVM environment get compiled down into byte code, which is interpreted by decompiler and it is abstracted in the way that only certain engineers with the knowledge can understand. We can eventually extract common elements into non technical and everyone can be a programmer of smart contracts.
- Running simulations is a large part of building proper smart contract systems. In the contect of layer one blockchain network, they have deep testing teams that spin up 100+ node networks, running different transaction, dispatching patterns over those networks, mutating the infrastructure, etc. There’s quite a lot of scope for having an AI augmented simulation.
- Is AI going to be a standardization execution tool or a standard setting tool? If it is a standard setting tool, are we going to create a risk where everyone is using old traditional inputs that dont have creativity? Should there be a focus on AI using the standards that humans have created as an execution? If yes, then we should avoid having automated smart contract creation agents since automated smart contract agents are actually limiting our ability.
- In the blockchain and AI spaces, trying to prescribe how things should be done has not really worked out so far. If we want to make it happen, there should be a coalition of blockchain foundations working together, combining resources, and making it happen from within the industry. If people in the blockchain space are going to use AI, they need to use it in a right way. Blockchain foundation should be proactive and take ethics more seriously generally.

3.11.Fireside with Q&A: How to Implement Privacy Pools

Date: Nov 21, 2023
Time: 10:30 - 11:15
Speaker:

- Jemma Xu (Portal Gate)
- Zooko Wilcox (Electric Coin Company)

Video: https://www.youtube.com/watch?v=FSuDw5Q-HqA
Summary:

- A smart contract-based privacy-enhancing protocol presented by Ethereum Founder Vitalik Buterin. A mechanism that allows legitimate users to separate themselves from transactions involving criminal activities while ensuring privacy by forming and mixing in groups, called "asocciation sets", consisting of only legitimate users.
- After a briefing by Jemma Xu, who develops and operates a protocol that applies a privacy pool called Dark Pool, a Q&A session was held with Zooko, one of the co-founders of ZCash. Zooko's key remarks were as follows:
    - We are concerned that the privacy pool proposed as a way for innocent users to prove their compliance with the law is a concept that is fundamentally contrary to the liberal democratic tradition, because in a liberal democracy, the principle of protecting innocent people from false accusations is more important than preventing crimes.
    - (In response to the point that it is very difficult to balance anonymity and transactions,) ZCash has a protocol that allows users to voluntarily and selectively disclose information about themselves, and the degree of disclosure is controllable.
    - Centralized exchanges can be seen as the dominant privacy solution in crypto assets, since users will be mixing with other customer assets when withdrawing funds.

3.12. Round Table 6: The Future of Wallet and Multi-Party Computation

Date: Nov 21, 2023
Time: 11:45 - 12:50
Speaker:

- Mitchell Travers (Soulbis, IKPWG Co-Chair)
- Daniel Goldscheider (Open Wallet Foundation)
- UV Hertzog (Tide Foundation)
- Angela Clark (Wallet Nation)
- Masato Yamanaka (SMTB and Georgetown University)

Video: https://www.youtube.com/watch?v=RClc8i-Ph0g&t=2s
Summary:

- MPC prevents cryptographic keys from residing in one place and allows them to reside nowhere else, depending on the group of participants. Each node participant has an incoherent piece of the cryptographic key, and the computation of the key can be performed without the group of nodes knowing what they are computing.

- The most significant outcome of MPC is that keys are correctly generated in a verifiable manner, used throughout their lifecycle, and managed to avoid cycling and lack of trust.

3.13. IKPWG Interactive Workshop Session 1: ZKP and its Applications

Date: Nov 21, 2023
Time: 13:45 - 15:15
Session Chair: Leona Hioki (Intmax)
Summary:

- Definition and Description of ZKP
    - Suppose there is a data lake that stores licenses, and some exchanges can share and crawl the license data, then the exchange proves that "I posess the license" without disclosing its license.
    - The difference between ZKP and FHE or other cryptography is that ZKP is a special Cryptography, but not Encryption.
- The traditional misconception about ZKP
    - With keywords like zkEVM, zkRollup, ..., etc. flying around, we feel very much that the definition, purpose and requirements are vague.
    - zkRollup focuses on scalability, but zk-application mainly focuses on privacy. Requirements for using ZKP vary depending on the purpose, but the public lumps them together.
    - Because of the gap between what can be constructed and what is available when considering legal processes, there is concern that on the one hand, technology will make it safe to use while protecting privacy, and on the other hand, analog methods using email, paper, and PDFs will accelerate. As a result, it would hinder the promotion of innovation.
    - ZKP performance is still in its infancy, so some user experience sacrifices must be made to protect privacy
- Sharing some interesting use cases about ZKP
- Developer Experience about ZKP
    - Currently, writing zkCircuit requires additional mathematical knowledge apart from existing web coding.
    - It isn't fast enough.
    - In some cases, users need to download certain files to their own desktops in order to generate a Proof.
    - Few documentations
    - To translate a statement to circuit, you need to dig through the GitHub documentation

3.14. IKPWG Interactive Workshop Session 2: Accountable Wallet

Date: Nov 21, 2023
Time: 13:45 - 15:15
Session Chair: Masato Yamanaka (SMTB and Georgetown University)
Summary:

- This paper focuses on the process of allowing legitimate users to avoid transacting with criminals with the use of an “Accountable Wallet”, a wallet with credentials that cryptographically ensure the holder’s privacy and prove that the holder meets the compliance requirements of the counterparty before any transaction. This paper addresses the challenges in implementing the process, related to the economic incentives of each player in the process and the reliability of credentials and their evaluation.
- Regarding what information credentials associated with a wallet should include, this paper suggests that a holder should prove the legitimacy of themselves, that of the wallet which they hold, and that of the cryptos which they transfer to their counterparty. This paper describes how and who issues those proofs.
- Based on the premise that the centralization of credential issuance is problematic, this paper suggests Decentralized Sanctions Screening Protocols, which enable the integration of multiple sanction lists in a decentralized manner.
- Even if the transaction itself between individuals is not illegal, the recipient may damage their legitimacy if the originator has been involved in any illegal activity in the past. Among participants, there was confusion about the current status of what is considered illegitimate activity, who is responsible, and how illegitimate activity is investigated and subsequently handled.
- The suggestion of this paper for dealing with the discovery of an originator’s past involvement in illegitimate activity after a transaction is for the recipient to evaluate the credentials of the originator before the transaction. Some participants, on the other hand, brought up the cancellation of the transaction as a solution, which seems not possible on the blockchain so far.
- There was an opinion that, while centralized exchanges prevent legitimate users from engaging in illegitimate activity by doing KYC and, if necessary, using investigation tools, it may be too much of a burden on individuals to expect them to take such measures in DeFi. The newest approach to reduce the burden of individuals can be the decentralized issuance of credentials, as suggested by this paper. However, there is also a point that decentralization is an unnatural state that requires ongoing effort and due diligence to keep it up.
- What this process protects legitimate users from is the receipt of cryptos from senders who have been involved in illegitimate activities in the past, and it does not intend to prevent legitimate users from passing funds to illegitimate users or allowing funds they pass to be used for illegitimate activities after the transaction. There was confusion about this point in the discussion.

3.15. IKPWG Interactive Workshop Session 3: Token and Privacy Impact: World Coin - Biometric Information

Date: Nov 21, 2023
Time: 15:30 - 17:00
Session Chair: Iris Rad (Clyde & Co.)
Summary:

- **Introduction to Worldcoin**: Introduced to the topic of privacy implications in biometric data collection and use. World Coin was introduced as a project focusing on proof of personhood using biometric information, specifically iris scanning.
- **Privacy and Ethical Concerns**: Discussed the privacy concerns related to collecting and using biometric data. Concerns from various data privacy commissions like Kenya's and France's were mentioned, highlighting the need for informed consent in data collection.
- **Technical and Security Aspects**: Discussed technicalities of the Worldcoin system, including how it uses a biometric scanning device (the orb) to scan a person's iris and issues a unique World ID. The security of such devices and the data storage practices were questioned, especially regarding the risk of data misuse or leakage.
- **Legal and Regulatory Perspectives**: Discussed legal perspectives, emphasizing the importance of complying with privacy and data protection laws. The panel highlighted that the usage of biometrics is not impossible from a privacy point of view but requires careful consideration of laws and ethical guidelines.
- **Utility and Application of Biometric Data**: Discussed the utility of biometric data in various sectors, including its application in cybersecurity for authenticating individuals in secure systems. The need for clear value exchange and consent in biometric data use was emphasized.
- **Public Perception and Awareness**: Pointed out that public perception plays a crucial role in the acceptance of biometric technology. They discussed the importance of educating the public about the privacy implications and the responsible use of biometric data.

3.16. IKPWG Interactive Workshop Session 3: Digital Identity - a global discourse

Date: Nov 21, 2023
Time: 15:30 - 17:00
Session Chair: Nat Sakimura (OpenID)
Summary:

- The definition of 'privacy' is ambiguous. Interpretation of the term varies among people. There are many kinds of privacy - data privacy, social privacy, etc.
- The vast amount of data that is being collected about you does not really matter. Information selling to you, customizing the news feed to you, and targeting propaganda towards you, might have a much bigger impact on your life than what everyone is worried about - a honeypot data. Data privacy can be taken from you without knowing and you can be a given target, being manipulated.

- Defining privacy is not productive. Adherence to privacy principles is the best approach for privacy. For example, the OECD privacy principles are a mandate to governments, and when it is applied to industry, you need to add something extra.
- What are key policy considerations surrounding digital identity on a global scale? How can they be harmonized to facilitate cross boarder interactions?
    - In the case of doing an identification, the outcome is different in every single case, since we need to know different things about different people. One of the missteps in our field was that the concept of digital identity is a very fluid and abstract concept - being any claim about a different subject.
    - The practice should be to really focus on the treatment of data problem. It is useful to boil down digital identity as data of a set of attributes. What do you need to know about somebody to do an identification? How are you going to know that? The best practice might be metadata. What we need is the subject in front of us and we need to be able to think about the metadata that tells us whether the subject is true or viable.
    - Your credit card number is never transmitted, and what is transmitted is a token that works only once. If regulation catches up, we should have AML things that should never know name, address, date of birth, and citizenship but basically just get a flag that says it is fine. Now there's a lot that needs to happen for that to work because someone needs to know such information. We need to have a process that is as secure as the one that we have today while still creating data minimization. Theoretically, it is good enough that you have six merchants and they all have different tokens. And the postal organization knows how to translate those tokens back into your info since if there is a data leak at the merchant, it just gets gibberish. (The most useful information for the AML process is physically where one exists in the world. If the bank not only does not have info on your PII and address but also does not understand the risk profile of you, your activities, and all of your other attributes and characteristics, how can the bank risk profile you being a customer? How can they understand you?)
- Data Minimization: What information do you need? Which should you acquire information itself or token? Data minimization is the limitation or processing of collected data, and such collected data should not be processed without tokenized.
- What would be the effective ways for multi-stakeholders to have this discourse continuously?
    - The efforts by the BGIN, the Open ID Foundation, and the Open Wallet Foundation can bring people together on all of three levels including regulations, specifications, and code.

3.17. Presentation: Introduction of NTT Digital

Date: Nov 22, 2023
Time: 9:45 - 10::00
Speakers: Eisuke Endo (NTT Digital)
Video: https://www.youtube.com/watch?v=LpuDy29HUD8

3.18. Industrial Round Table 1: Toward Sound Blockchain-based Financial System

Date: Nov 22, 2023
Time: 10:00 - 11:00
Speakers:

- Mark Greenslade (Head of R&D @Casper Association)
- Matthew Doty (R&D Consultant @Casper Association)
- Lulio Vargas-Cohen (Circle)
- Jumpei Miwa (Recruit)
- Hiromi Yamaoka (DeCurret DCP)

Video: https://www.youtube.com/watch?v=VGCwoOdLXa0

3.18. Industrial Round Table 2: Blockchain for Trustworthiness of Digital Society

Date: Nov 22, 2023
Time: 11:30 - 12:30
Speakers:

- Ken Katayama (NRI)
- Joi Ito (Digital Garage)
- Final Aim

Video: https://www.youtube.com/watch?v=eWMIT3iHzBg

3.18. Speech: Blockchain-enabled Digital Government: Innovation, Application, and Strategic Value Co-Creation

Date: Nov 22, 2023
Time: 13:30 - 14:00
Speakers: Dr. Dimitrios Salampasis
Video: https://www.youtube.com/watch?v=lZOzRU31uiY

3.19. Fireside Chat: Discovering the Australian Blockchain Collaboration Opportunity

Date: Nov 22, 2023
Time: 11:30 - 12:30
Speakers:

- Michael Bacina (Piper Alderman)
- Simon Callaghan (Blockchain Australia)
- Rob Allen (Australian Payments Plus)
- Mitchel Travers (Soulbis)

Video: https://www.youtube.com/watch?v=oHyIXr98NcQ
Summary:

- Questions that were discussed
    - What are the key policy considerations that can foster collaboration and innovation in the Australian blockchain sector, and how do they align with broader economic and technological objectives?
    - Can you provide insights into the current state of the Australian blockchain landscape, including industry strengths, challenges, and areas for growth?
    - How does academic research contribute to the understanding and development of blockchain technology in Australia, and what specific areas of study hold promise for future innovation?
    - What role does industry collaboration play in advancing blockchain solutions, and can you share successful examples of such collaborations in the Australian context?
    - Are there regulatory frameworks and standards that can facilitate blockchain adoption and interoperability, and what is the industry's perspective on these issues?
    - How can Australian blockchain initiatives contribute to global blockchain ecosystems and standards, and what are the potential benefits of international collaboration?
    - Can you share specific use cases or projects in Australia that demonstrate the real-world impact and potential of blockchain technology?
    - In what ways does blockchain innovation intersect with the Australian Payments Plus initiative, and how can blockchain enhance payment systems and financial services in the country?

3.20. LightLink - Scaling to Millions (15 mins) Presentation

Date: Nov 22, 2023
Time: 14:30 - 14:45
Speakers:

- Roy Hui (LightLink)

Video: https://www.youtube.com/watch?v=qcGqUgsR58U

3.20. Australia’s Position in the Global Blockchain Industry

Date: Nov 22, 2023
Time: 14:45 - 15:00
Speakers:

- Steve Vallas (Blockchain APAC)
- Michael Bacina (Piper Alderman)

Video: https://www.youtube.com/watch?v=kpSrAkYTwHU&t=1s

3.21. Fireside Chat: Decentralized Foundations: Globally Organizing Strangers

Date: Nov 22, 2023
Time: 16:00 - 16:45

Speakers:

- Mehdi Zerouali
- Anthony Sassano

Video: https://www.youtube.com/watch?v=l3GWv5e2fSg

Summary:

- Questions that were discussed
  - How do governance models in decentralised foundations differ from traditional organisational structures?
  - How do decentralised foundations build trust and foster community among global participants who may never meet in person?
  - What are the primary challenges faced in coordinating efforts and decision-making processes in a global, decentralised environment?
  - What communication strategies are most effective in maintaining clear and consistent dialogues within decentralised foundations?
  - How do decentralised foundations ensure inclusivity and representation of diverse voices in their operations and decision-making?
  - How sustainable is the decentralised foundation model, especially in terms of scalability and adaptability to changing environments?
  - Can you share any success stories or key learnings from your experiences with decentralised foundations?
  - What do you envision for the future of decentralised foundations, especially in the context of evolving digital technologies?

4. Financial Report

4.1. Incomes

Event Sponsor Fee:	3,500,000 JPY
Event Ticket:	1,284,794 JPY (8,619.89 USD, as of Nov 20, 2023)
Total	4,784,794 JPY

4.2. Expenditures

Venue Rental	1,665,900 JPY (17,116 UD, as of Nov 20, 2023)
Catering	214,967 JPY (2,208.64 AUD, as of Nov 20, 2023))
Audio & Visual	1,143,841 JPY (11,752.19 USD, as of Nov 20, 2023)
Banner and design	40,302 JPY (414.08 AUD, as of Nov 20, 2023)
Travel Support (WG Co-chairs, Keynote Speaker and Staff)	1,037,310 JPY
Transfer to BN for its operation costs	682,474 JPY
Total	4,784,794 JPY

5. Future General Meetings

The next general meeting (Block #10) will be held from Mar 3, 2024 to Mar 6, 2024 in Tokyo, Japan.

6. Block #9 Organizers, BGIN and Working Group Chairs

- BGIN Co-Chairs
    - Shin'ichiro Matsuo
    - Mai Santamaria
- Working Group/Task Force Co-Chairs
    - Nat Sakimura
    - Mitchell Travers
    - Leon Molchanovsky
    - Chloe White
- Local organizers
    - Joseph Beverley
    - Steve Vallas
    - Joshua Landua
    - Chloe White
    - Richelle Cox
- Co-Chair of the previous block (Block #8)
    - Andrea Bracalli
- Co-Chair candidate of the next block (Block #10)
    - Jumpei Miwa
- Administration
    - Takaya Sugino
    - Masato Tsutsumi
    - Lulu Ito