BGIN Meeting Report

Date: TBD
Location: Virtual Meeting

Executive Summary

The meeting discussed the structure and scope of a global competition for post-quantum cryptography (PQC) migration in blockchain systems, particularly focusing on Bitcoin and Ethereum. Key points included:

1. **Scope and Objectives**:
   - The competition aims to develop governance mechanisms and technical solutions for PQC migration.
   - It will involve designing and implementing new protocols or software to incorporate NIST-certified post-quantum signatures into blockchains.
2. **Call for Papers**:
   - A call for papers will be published in August~~in August~~, with a deadline in late August.
   - The symposium will take place in October, focusing on information security and blockchain technology.
3. **Global Testbed**:
   - A global testbed will be set up to evaluate the transition of blockchain data.
   - The Japanese government and N~~AT~~EDO~~O~~ will provide initial funding, with additional nodes potentially contributed by other organizations.
4. **Node Requirements**:
   - Discussions are ongoing to determine the number of nodes needed for a fair evaluation.
   - Collaboration with entities like the Ethereum Foundation is being considered to secure sufficient nodes.
5. **Next Steps**:
   - Input from participants via email or discourse channels is encouraged.
   - The next key event will be the symposium in October, where progress towards the competition's start will be advanced.

The meeting focused on organizing a comprehensive competition and symposium centered around post-quantum cryptography (PQC) migration for Bitcoin and Ethereum, with an emphasis on both technological and governance aspects. Key topics included the socialization of the call for papers, determination of node requirements for the evaluation test, organization of the blockchain workshop in Shizuoka prefecture, and collaboration with global universities and organizations. The call for papers is set to be published by the first week of August, with a submission deadline in late August. The competition will

explore mechanisms that support cryptographic agility and PQC readiness, balancing short-term risk mitigation with long-term security. The symposium, scheduled for the last week of October, will include discussions on PQC migration and cryptographic agility.

Key decisions included setting up an initial 10 evaluation nodes funded by the Japanese government, with plans to add more nodes through collaboration with other organizations such as the Ethereum Foundation. Participants agreed on the importance of a fair and representative evaluation process, ensuring that nodes are distributed across different regions (e.g., Asia, Europe, North America). The meeting also emphasized leveraging global expertise and funding sources to enhance the competition's effectiveness. Overall, the outcomes underscore the significance of fostering international collaboration and advancing cryptographic practices to ensure blockchain systems remain secure in the face of quantum computing threats.

Key Discussion Points

1. **Socialize Call for Papers**
   - The call for papers will be published by the first week of August.
   - Submissions are due in the third or fourth week of August.
   - The call for papers will be available in both Japanese and English to encourage global participation.
2. **Determine Node Requirements**
   - Work with stakeholders to determine the appropriate number of nodes needed for a fair evaluation test.
   - Initially, plan to set up 10 nodes for a six-month period.
   - Collaborate with other organizations, such as the Ethereum Foundation, to secure additional nodes if necessary.
   - Ensure a balanced distribution of nodes (e.g., 3 in Asia, 5 in Europe, 5 in North America) to ensure a fair and representative evaluation.
3. **Organize Symposium**
   - Plan the blockchain workshop (BWS) in Shizuoka prefecture, Japan, during the last week of October.
   - The symposium will include discussions on post-quantum cryptography (PQC) migration and cryptographic agility.
4. **Collaborate with Universities**
   - Collaborate with global universities to operate the evaluation test more effectively.
   - Leverage Japanese government budget and other funding sources to set up and maintain evaluation nodes.
5. **Scope of the Competition**
   - The competition will focus on post-quantum migration for Bitcoin and Ethereum, covering ~~both~~ technological aspects (e.g., implementing new signature schemes)~~ and governance aspects (e.g., designing a fair transition period)~~.

- Balance short-term solutions that mitigate immediate risks with long-term solutions that ensure sustained security.

6. **Cryptographic Agility vs. PQC Readiness**
   - Cryptographic agility involves designing systems that can easily switch between different cryptographic algorithms.
   - While achieving cryptographic agility is more challenging than PQC readiness, it is crucial for future-proofing blockchain systems.
   - The competition should explore mechanisms that support various policies and are flexible enough to adapt to new threats.
7. **Evaluation Test**
   - The Japanese government will provide some budget to set up evaluation nodes.
   - Initially, the plan is to set up 10 nodes for a six-month period.
   - Additional nodes can be added through collaboration with other organizations.
   - Determine the appropriate number of nodes to ensure a fair and representative evaluation.
8. **Call for Papers**
   - The call for papers will address various aspects of PQC migration, including technical proposals, governance models, and policy considerations.
   - Submissions should be encouraged from global participants to gather diverse perspectives and solutions.
   - The symposium in October will provide a platform to discuss and advance the competition's progress.
9. **Next Steps**
   - Finalize the number of nodes needed for the evaluation test.
   - Collaborate with other organizations to secure additional nodes.
   - Socialize the call for papers and encourage submissions from global participants.
   - Prepare for the symposium in October to finalize the scope and criteria of the competition.

~~10. **Personhood Paper**~~
   - ~~The meeting did not explicitly discuss a "Personhood Paper," but it is important to note that discussions on personhood, identity, and related ethical considerations could be relevant to future workshops or papers within the broader context of blockchain and PQC.~~

~~11. **Taxonomy of Harms**~~
   - ~~The meeting did not explicitly discuss a "Taxonomy of Harms" or FASE, but these concepts are crucial for understanding and mitigating risks in the transition to post-quantum cryptography. Future discussions should consider categorizing potential harms and developing strategies to address them.~~

~~12.~~10. **Understanding is Key**

- The meeting emphasized the importance of clear communication and understanding among participants.
- Proverbs and wisdom from various cultures, such as the one related to Zcash, highlight the need for transparency and collaboration in blockchain and PQC initiatives.

Action Items and Next Steps

1. **Call for Papers Preparation**:
   - Prepare and publish the call for papers by early August.
   - Set a deadline for submissions in late August.
2. **Symposium Organization**:
   - Finalize details for the blockchain workshop symposium in October.
   - Ensure the event is promoted to attract international participation.
3. **Testbed Setup**:
   - Determine the number of nodes required for a fair evaluation.
   - Secure funding and collaboration from various organizations to set up the testbed.
4. **Node Collaboration**:
   - Engage with entities like the Ethereum Foundation to contribute nodes.
   - Ensure the testbed is globally distributed to accurately represent blockchain networks.
5. **Input Collection**:
   - Collect input on node requirements and competition scope via email or discourse channels.
   - Provide updates and feedback to participants regularly.

Discussion Points

1. **Governance vs. Technical Solutions**:
   - The need to balance governance mechanisms with technical solutions in the competition was emphasized.
   - Participants discussed whether the focus should be solely on PQC migration or include broader crypto agility considerations.
2. **PQC Signature Schemes**:
   - The assumption that NIST-certified post-quantum signatures are already available and do not need reinvention.
   - Discussion on how to effectively incorporate these schemes into blockchain systems.
3. **Short-term vs. Long-term Solutions**:
   - Consideration of both short-term and long-term effectiveness in PQC solutions.
   - The importance of rewarding practical, short-term solutions while also supporting more complex, long-term strategies.
4. **Policy and Mechanism Support**:

- The role of policy and mechanism design in supporting various blockchain protocols and policies.
- Discussion on the range of policies that should be supported or accepted for the competition.

5. **Testbed Evaluation**:
   - The importance of a globally distributed testbed to accurately evaluate PQC migration.
   - Budget constraints and the need for collaboration to secure sufficient nodes.

~~**Attendees**~~

- ~~Ito-san~~
- ~~Suga-san (Organizer of the Blockchain Workshop)~~
- ~~Keegan (Ethereum Foundation)~~
- ~~Andy (Remote Participant, NIST)~~
- ~~Various other participants from Japanese government, NATO, and global universities.~~

~~Detailed Session Summary~~

1. ~~**Call for Papers Preparation**:~~
   - ~~Prepare and publish the call for papers by early August.~~
   - ~~Set a deadline for submissions in late August.~~
2. ~~**Symposium Organization**:~~
   - ~~Finalize details for the blockchain workshop symposium in October.~~
   - ~~Ensure the event is promoted to attract international participation.~~
3. ~~**Testbed Setup**:~~
   - ~~Determine the number of nodes required for a fair evaluation.~~
   - ~~Secure funding and collaboration from various organizations to set up the testbed.~~
4. ~~**Node Collaboration**:~~
   - ~~Engage with entities like the Ethereum Foundation to contribute nodes.~~
   - ~~Ensure the testbed is globally distributed to accurately represent blockchain networks.~~
5. ~~**Input Collection**:~~
   - ~~Collect input on node requirements and competition scope via email or discourse channels.~~
   - ~~Provide updates and feedback to participants regularly.~~

~~**Discussion Points**~~

1. ~~**Governance vs. Technical Solutions**:~~
   - ~~The need to balance governance mechanisms with technical solutions in the competition was emphasized.~~
   - ~~Participants discussed whether the focus should be solely on PQC migration or include broader crypto agility considerations.~~

2. **PQC Signature Schemes**:
   - The assumption that NIST-certified post-quantum signatures are already available and do not need reinvention.
   - Discussion on how to effectively incorporate these schemes into blockchain systems.
3. **Short-term vs. Long-term Solutions**:
   - Consideration of both short-term and long-term effectiveness in PQC solutions.
   - The importance of rewarding practical, short-term solutions while also supporting more complex, long-term strategies.
4. **Policy and Mechanism Support**:
   - The role of policy and mechanism design in supporting various blockchain protocols and policies.
   - Discussion on the range of policies that should be supported or accepted for the competition.
5. **Testbed Evaluation**:
   - The importance of a globally distributed testbed to accurately evaluate PQC migration.
   - Budget constraints and the need for collaboration to secure sufficient nodes.

Attendees

- Ito-san
- Suga-san (Organizer of the Blockchain Workshop)
- Kigeneegan (Remote Participant, Virginia TechEthereum Foundation)
- Andy (Remote Participant, NIST)
- Various other participants from Japanese government, NEDOATO, and global universities.

The meeting focused on organizing a comprehensive competition and symposium centered around post-quantum cryptography (PQC) migration for Bitcoin and Ethereum, with an emphasis on both technological and governance aspects. Key topics included the socialization of the call for papers, determination of node requirements for the evaluation test, organization of the blockchain workshop in Shizuoka prefecture, and collaboration with global universities and organizations. The call for papers is set to be published by the first week of August, with a submission deadline in late August. The competition will explore mechanisms that support cryptographic agility and PQC readiness, balancing short-term risk mitigation with long-term security. The symposium, scheduled for the last week of October, will include discussions on PQC migration and cryptographic agility.

Key decisions included setting up an initial 10 evaluation nodes funded by the Japanese government, with plans to add more nodes through collaboration with other organizations such as the Ethereum Foundation. Participants agreed on the importance of a fair and representative evaluation process, ensuring that nodes are distributed across different regions (e.g., Asia, Europe, North America). The meeting also emphasized leveraging global

expertise and funding sources to enhance the competition's effectiveness. Overall, the outcomes underscore the significance of fostering international collaboration and advancing cryptographic practices to ensure blockchain systems remain secure in the face of quantum computing threats.

1. **Socialize Call for Papers**
   - The call for papers will be published by the first week of August.
   - Submissions are due in the third or fourth week of August.
   - The call for papers will be available in both Japanese and English to encourage global participation.
2. **Determine Node Requirements**
   - Work with stakeholders to determine the appropriate number of nodes needed for a fair evaluation test.
   - Initially, plan to set up 10 nodes for a six-month period.
   - Collaborate with other organizations, such as the Ethereum Foundation, to secure additional nodes if necessary.
   - Ensure a balanced distribution of nodes (e.g., 3 in Asia, 5 in Europe, 5 in North America) to ensure a fair and representative evaluation.
3. **Organize Symposium**
   - Plan the blockchain workshop (BWS) in Shizuoka prefecture, Japan, during the last week of October.
   - The symposium will include discussions on post-quantum cryptography (PQC) migration and cryptographic agility.
4. **Collaborate with Universities**
   - Collaborate with global universities to operate the evaluation test more effectively.
   - Leverage Japanese government budget and other funding sources to set up and maintain evaluation nodes.
5. **Scope of the Competition**
   - The competition will focus on post-quantum migration for Bitcoin and Ethereum, covering both technological aspects (e.g., implementing new signature schemes) and governance aspects (e.g., designing a fair transition period).
   - Balance short-term solutions that mitigate immediate risks with long-term solutions that ensure sustained security.
6. **Cryptographic Agility vs. PQC Readiness**
   - Cryptographic agility involves designing systems that can easily switch between different cryptographic algorithms.
   - While achieving cryptographic agility is more challenging than PQC readiness, it is crucial for future-proofing blockchain systems.
   - The competition should explore mechanisms that support various policies and are flexible enough to adapt to new threats.
7. **Evaluation Test**

- The Japanese government will provide some budget to set up evaluation nodes.
- Initially, the plan is to set up 10 nodes for a six-month period.
- Additional nodes can be added through collaboration with other organizations.
- Determine the appropriate number of nodes to ensure a fair and representative evaluation.

8. **Call for Papers**
   - The call for papers will address various aspects of PQC migration, including technical proposals, governance models, and policy considerations.
   - Submissions should be encouraged from global participants to gather diverse perspectives and solutions.
   - The symposium in October will provide a platform to discuss and advance the competition's progress.
9. **Next Steps**
   - Finalize the number of nodes needed for the evaluation test.
   - Collaborate with other organizations to secure additional nodes.
   - Socialize the call for papers and encourage submissions from global participants.
   - Prepare for the symposium in October to finalize the scope and criteria of the competition.
10. **Personhood Paper**
    - The meeting did not explicitly discuss a "Personhood Paper," but it is important to note that discussions on personhood, identity, and related ethical considerations could be relevant to future workshops or papers within the broader context of blockchain and PQC.
11. **Taxonomy of Harms**
    - The meeting did not explicitly discuss a "Taxonomy of Harms" or FASE, but these concepts are crucial for understanding and mitigating risks in the transition to post-quantum cryptography. Future discussions should consider categorizing potential harms and developing strategies to address them.
12. **Understanding is Key**
    - The meeting emphasized the importance of clear communication and understanding among participants.
    - Proverbs and wisdom from various cultures, such as the one related to Zcash, highlight the need for transparency and collaboration in blockchain and PQC initiatives.

Appendix: Full Meeting Transcript (Anonymized)

3.0 --> 8.3: So, this is the Crypto Agility and PQC migration session.
8.7 --> 15.3: We just heard an announcement from Meti on the blockchain competition or the PQC competition.
16.9 --> 23.1: It will start next year and the goal is to progress post-quantum cryptography and ensure
23.1 --> 26.5: that all of our digital assets and blockchain is safe long term.
27.4 --> 36.5: We have a lot of work to do to ensure that the competition is fair and is taking in all
36.5 --> 45.8: of the different techniques and pathways that are possible for PQC and that's going to be
45.8 --> 52.2: a center of Begin's work for the next year is coming up with that criteria for the competition
52.7 --> 63.3: as well as navigating the PQC academics and market for different options and then guiding those
66.8 --> 73.7: groups towards the competition this time next year. So, there was a timeline shared.
74.3 --> 81.5: The timeline and the most immediate outcome that we're discussing is a collection of papers and
81.5 --> 88.4: research and groups to announce and share that this competition is happening and that will happen
88.4 --> 98.5: in April and then I assume the pathway from there until block 15 is to then share and discuss the
98.5 --> 109.7: criteria within the IKP working group for PQC and then make more concrete announcements or
110.3 --> 119.8: descriptions of the competition in block 15 to then follow on to block 16 this time next year
119.8 --> 129.0: and hopefully the competition is all steam ahead at that point and we're discussing and
129.0 --> 138.1: making advancements on the techniques that are required to again PQC. So, do you want to go maybe
138.1 --> 152.2: next slide? Is Keegan online? Yes, I'm here. Should we get started with his presentation then?
159.0 --> 159.8: Yeah, I can.
162.1 --> 166.4: Should I? Okay. Yeah, if you can share your screen when you're ready. All right.
168.9 --> 171.7: Then let me share the screen.
174.3 --> 176.2: No, this is the one.
182.3 --> 184.1: Okay, I hope you guys can see the screen.
187.7 --> 193.6: Yeah, we can. All right. Okay, let me start my presentation as a kickoff
193.6 --> 200.8: presentation for this session. I'm trying not to spend too much time and leave enough time for
200.8 --> 207.9: discussion for the competition, but this presentation is kind of aiming to give the
207.9 --> 213.1: fundamental, I mean common understanding, what the structure of the problem is and what
213.1 --> 221.4: we're trying to solve through the competition. Anyway, I'm

Keegan Fukuda from
221.4 --> 227.2: Virginia Tech, and this is the presentation title, the Bloc kchain PQC Transition Landscape.
228.8 --> 233.7: And, well, like, you know, background, I think I'm not gonn a, I don't really have to cover this, but
234.3 --> 238.7: you know, the cryptographic primitives, you know, foundatio nal to blockchain, like, you know,
238.8 --> 243.7: digital signature are not threatened by the cryptographical ly relevant quantum computer,
244.2 --> 250.1: CRQC in short. And, you know, quantum attacker may derive t he sign-in key from the verification
250.1 --> 255.6: key and, you know, force about its signature and execute th e unauthorized asset transfers. So, like,
255.8 --> 262.1: the, you know, blockchain core principle, like, not your ke y, not your coins, will never stand
262.1 --> 269.1: anymore after the Q&A. And so, the PQC migration is what, I mean, the necessity for the PQC
269.1 --> 273.4: migration is widely acknowledged, but the blockchain remain s an extremely, you know,
273.4 --> 278.3: challenging domain for the, this kind of migration, because, like, there's, first of all,
278.3 --> 286.1: no centralized administrator responsible for handling the m igration. And also, like, the impact
286.1 --> 293.0: of the compromised digital signature or other primitives is really catastrophic, because,
293.2 --> 300.3: you know, blockchain is a financial system in the end anywa y. And also, like, on-chain data
300.9 --> 306.9: may require the extremely long-term validity, could be. And also, the most important
306.9 --> 314.0: and the most difficult problem I see is the, you know, misa ligned incentives and the conflicting
314.0 --> 319.5: speculation amongst stakeholders. So, like, the reaching co nsensus in the PQC migration is quite
319.5 --> 325.7: difficult. So, there's kind of a little beef happened on th e Twitter. Oh, X, right now, X.
327.1 --> 332.6: Last year, like, the venture capitalist Nick Carter was, yo u know, publishing some reports,
333.1 --> 338.5: alerting the spread of the quantum computer for Bitcoin com munity, and saying, like, Bitcoin
338.5 --> 347.9: community is completely ignoring this risk. And the Adam Ba ck from Blockstream, you know, refute
347.9 --> 355.4: against it, like saying, you know, we are very, I mean, we are now on the right stage of the
355.4 --> 362.2: preparation for the PQC transition, and don't try to move y our market. Because, you know,
362.2 --> 367.5: looking at the Nick Carter's portfolio, he's investing mone y to the, you know, startup called
367.5 --> 373.0: Project 11, which is selling the, like, some tool supportin g the PQC migration for blockchain.
373.6 --> 379.2: So, like, you know, anyway, this discussion is always flagm

ented because of this, you know,
379.5 --> 386.8: underlying, like, financial incentives and so on. And even the individual stake, even the individual,
386.8 --> 393.1: you know, like, investors really care about the, you know, asset price for sure,
393.3 --> 399.8: and the PQC migration will definitely affect it. So, again, like this, financial incentives,
400.2 --> 404.8: but the other incentives to, you know, this effect on, like, you know, individual level
404.8 --> 413.4: and the organizational level and so on. And so, and the impact and threat of the CRQC
413.4 --> 421.0: remains really unorganized yet. And especially, you know, again, you know, compared to the
421.6 --> 428.9: very early stage of the blockchain, like now in 2026, diverse stakeholders and their incentives
428.9 --> 433.4: have become really complex. So discussion within the academia and the blockchain community have
433.4 --> 438.1: become really fragmented. And there's no comprehensive framework exists that, you know,
438.1 --> 444.8: enable the technical and governance challenges. And that's why I do this work.
445.3 --> 450.7: And actually, okay, actually, this work is presented at the NIST Crypto Agility Workshop
450.7 --> 457.6: at first that happened in 2025, April something. And this topic is chosen in, you know,
458.4 --> 464.5: for, you know, 10 presentations throughout two days. And so this is quite important topic,
464.5 --> 473.0: which, you know, even NIST really focused, really interested in. And, well, in this
473.0 --> 478.9: presentation, I really covered, you know, broader aspect of the difficulties in the
479.7 --> 484.6: blockchain piggies migration, but this presentation will quite focus on the,
484.8 --> 490.3: again, the incentive side, the intertwined incentive of the stakeholders. But again,
491.0 --> 496.8: don't really have time to cover everything I researched. So please, I mean, if you're
496.8 --> 501.8: interested, please read the QR code that will guide you to the eprint archive paper.
503.4 --> 509.2: Anyway, so before moving on to the governance aspect of the difficulties, let me cover
509.2 --> 514.7: briefly the technical difficulties first. I mean, maybe some of them are quite obvious. But first
514.7 --> 524.1: of all, the biggest problem is the increased signature size and key size. So ECDSA on Bitcoin
524.1 --> 532.9: verification, on Bitcoin, the verification key is 33 byte and signature is 77 byte. On the other
532.9 --> 537.9: hand, Falcone, which is, you know, one of the most top candidates for, you know, those blockchain
537.9 --> 546.9: community to use for the PQC signature. Its verification ke

y is like 897 byte, signature is
547.7 --> 554.8: 666 byte, which is quite bigger, obviously. And needless to say, the tradeoff between the
554.8 --> 560.6: throughput and the decentralization exists in blockchain. So, I mean, if we increase the block
560.6 --> 564.7: size corresponding to the bigger, you know, key size, and that's going to be a problem for the
564.7 --> 571.7: decentralization, and vice versa. And some mitigation plans for this, you know, large key
571.7 --> 576.4: size is proposed, but none of them are fundamentally solving this, you know, tradeoff.
577.3 --> 583.8: And also, like, you know, there should be migration, the migration should cover, you know,
583.8 --> 589.7: the other primitives other than, you know, transaction signing algorithm, like, you know,
589.7 --> 595.7: signature aggregation, also the other primitives, like polynomial commitment, scaling solution,
595.9 --> 602.7: smart contracts. So all like, you know, those primitives quite depends on each chain instance.
603.0 --> 610.1: So like each chain instance, Bitcoin, Ethereum, Solana, etc. I mean, those, I mean, each chain
610.1 --> 616.8: requires rigorous analysis of their own risk and, you know, their own like necessity for the PQC
616.8 --> 627.2: migration. Okay, so after that, let me dive into the stakeholder incentive analysis. So this is
627.9 --> 636.2: here I list like five to six stakeholders, very simplified incentive descriptions,
637.2 --> 646.9: especially this case is like, assuming the Bitcoin case, the user here, the first their interest is
646.9 --> 652.6: the minimizing the economic and the operational cost within the migration. And blockchain
652.6 --> 659.5: ideologists, like Bitcoin, or developers, they want to preserve the decentralization
659.5 --> 666.0: nature. And that's their first priority. And the miners, they want to maintain the profitability
666.0 --> 672.8: and the maximize the total transaction fee revenue within the migration. And the investors,
673.2 --> 678.4: they prioritize short term asset price and the, you know, pursue the long term profits. Again,
678.5 --> 684.2: I mean, there should be much more broader, much broader, you know, their strategies. But here,
684.2 --> 693.2: let me just simplify those strategies and so on. And node operators, they want to avoid the,
693.2 --> 696.8: you know, increases in the operational overhead, like such as higher computational
696.8 --> 703.5: resource requirements, or higher storage costs to run the full node. And lastly,
704.4 --> 708.9: I named collect collective interest, but that's basically the interest for everyone.
709.6 --> 714.0: They want, we want to avoid forks to ensure the robust secu

rity and the preserve the
714.0 --> 723.1: overall value of the asset. And after that, okay, given tha t, let me go over the,
723.9 --> 730.2: like some of proposed transaction migration, transaction si gning algorithm migration plan
731.6 --> 738.2: that I found in both in academia and blockchain community. So the first two cases I'm going to
738.2 --> 745.2: cover is the first one, the legacy secret, I'll keep the pl an keep using a legacy secret
745.9 --> 750.4: by using the post quantum general knowledge proof. Here, th e legacy secret is the mnemonic
750.4 --> 756.3: code of the signing key, basically the pre image of the sig ning key. So that's going to be quantum
756.3 --> 764.1: secure, even after QA, because, you know, it's the digest, the hash digest of mnemonic code will
764.1 --> 769.0: eventually become the signing key. So it's not, it's not to be kept safe after the quantum
769.0 --> 778.6: computer. And like, as long as the user keeps this mnemonic code in secret, then that can be used as
778.6 --> 783.8: the, you know, secret information for signing, that's their core idea. And we can expect, you
783.8 --> 788.3: know, shorter migration period for this case, because these are don't really have to generate
788.3 --> 792.4: a new key. And these are don't really have to, you know, is sue the transaction to move the fund.
793.0 --> 799.0: And on the other hand, I mean, that the similar case, not v ery similar, but I classified similar
799.9 --> 805.9: is the using the hybrid signature and the account of obstru ction. So what I do is,
806.5 --> 812.7: they'll require, you know, incorporating the post quantum s ignature, but at the same time,
813.4 --> 820.2: let the user keep using the traditional ECDSA secret at the same time. So it's going to ensure
820.2 --> 825.8: the backward compatibility, user can keep using the same ke y. And in this case, the,
827.2 --> 832.6: even the user are required to generate the post quantum sig nature key.
833.8 --> 840.4: Now user can also at the same time keep using the ECDSA key. So maybe they don't really have to,
840.4 --> 846.5: you know, move the fund from the plastic address to the new address. But the maybe we can keep
846.5 --> 851.4: the other system same before and after the migration. Anywa y, so in these cases,
852.4 --> 857.3: the end users will have less burden in the transaction migh t, I'm sorry, in the migration,
857.9 --> 863.4: and node operators and developers are having more cost, bas ically incurring the overhead,
863.9 --> 869.9: because anyway, the verification of the ZKP, also like, you know, implementing and maintaining both
869.9 --> 879.0: plastic signature and post quantum signature is like, costl

y. And backward compatibility is
879.0 --> 886.7: ensured in both cases. So it will avoid a fork, hopefully, and also miners will gain no profit,
887.1 --> 895.0: because again, there's no migration transaction required in these plans. And on the other hand,
895.0 --> 905.1: uh, this is the most naive migration plan that I call pure PQC. So this is the migration to the
905.1 --> 910.4: completely new address system. So it requires you to simply generate the post quantum signing key
910.4 --> 916.7: and also generate the address and they require the user to move the fund from the classical
916.7 --> 922.7: address to the new address. So the user will have more burden in the migration, but node operators
922.7 --> 927.8: and developers will have less cost. That means like, it's, I mean, much more simpler than the
927.8 --> 935.8: last two migration plans. And there are no backward compatibilities and that
937.5 --> 944.3: resulting in the high probabilities of the fork, high probabilities of the fork, and miners will
944.3 --> 951.0: gain some profit, you know, because all user will eventually require to issue the transaction
951.7 --> 959.9: for migration. The last one, the third one is the, that I call migration by centralization.
960.6 --> 969.9: So here I found some like plan like saying, uh, let's have the emergency rollback in case we find
969.9 --> 977.8: like any quantum attack. And so we basically roll back the chain and, uh, move to the post
977.8 --> 984.7: quantum signature or whatever, uh, after that block, that is one plan actually. And the other
984.7 --> 991.1: plan is the quantum resistant proxy. That is like, uh, they implement some proxy signature,
991.5 --> 996.4: uh, like proxy smart contract, you know, implementing the quantum signature so that
996.4 --> 1002.0: user can use that contract as a vault, a quantum secure vault, and they can, you know,
1002.0 --> 1008.6: temporarily deposit their asset there and withdraw it later. Uh, that's, that's how they want to
1008.6 --> 1015.9: proceed, um, the migration. Anyway, these plan, uh, this decentralization and compromise anyway,
1015.9 --> 1020.3: because, you know, either, either of them, um, making the single point of failure,
1020.8 --> 1025.6: but we can expect the short migration period and also less overhead.
1027.1 --> 1035.5: So by covering all, you know, these migration plans proposed, uh, especially in case of Bitcoin,
1035.9 --> 1045.8: we can see the tremendous relationship in this, in these plan. So, excuse me. So when over,
1045.9 --> 1053.6: when we incur overhead and the simplicity is sacrificed, then we can have the phased migration
1053.6 --> 1059.1: as we saw at the first case. So the decentralization and

the security is ensured
1059.1 --> 1065.1: because it maintains the backward compatibility. And also that's, that's ensuring the seamless
1065.1 --> 1074.2: transition and the less risk of forks. And by having the centralized authority power or decision
1074.2 --> 1082.7: making, then we can ensure the security overhead because, uh, you know, that ensure the rapid
1082.7 --> 1089.5: migration and that, you know, short, shorter window, uh, minimize the duration of the exporter
1089.5 --> 1097.0: of the security vulnerabilities. And again, it's gonna ha ve no overhead. And if we decide to take
1097.0 --> 1102.2: the naive way, uh, in the prioritizing both decentralizat ion and overhead, then that's
1102.2 --> 1110.9: going to risk the security because it will end up as the autonomous and incremental migration.
1110.9 --> 1115.6: So that is time consuming and, you know, carries a high r isk of the chain forks
1116.1 --> 1119.8: and, you know, hashrate fragmentation during the transiti on double, you know,
1119.9 --> 1127.6: eventually, uh, risk the security of the chain. And this dilemma is, I'm sorry, this dilemma is,
1127.9 --> 1135.9: uh, relation relationship can be found in specific, uh, c ases. Like for example,
1135.9 --> 1142.4: the dilemma of the Dorban asset. So the Dorban asset is t he asset that are not expected to be
1142.4 --> 1148.5: migrated, uh, during the migration period, maybe for some reason, like, uh, the owner has passed
1148.5 --> 1156.4: away or simply they lost the signing key. And there are t wo approaches for this asset to like,
1156.6 --> 1163.0: one is the mandatory migration. So they set the specific deadline for the migration and completely
1163.0 --> 1170.4: reject the plastic transaction after that period. Uh, so that, you know, they can be prepared before
1170.4 --> 1174.5: the QA happens, but the other case is the maintaining the backward compatibility.
1174.9 --> 1180.6: So it's going to allow, uh, the transaction of the classi c signature signature, even after QA.
1180.8 --> 1188.4: So those dilemma, uh, those Dorban asset will be stolen b y a doctor after the QA, uh, in this case.
1188.4 --> 1198.9: And this, uh, uh, monitoring migration is almost freezing the, uh,
1199.7 --> 1203.7: Dorban asset. So that's kind of getting the crits getting criticized as the,
1204.4 --> 1208.2: uh, like, you know, as damaging the core principle of the blockchain,
1208.3 --> 1213.3: like censorship resistance. So it's gonna sacrifice in th e decentralization in this
1213.3 --> 1218.5: dilemma, but, uh, this backward compatibility plan is all owing the
1218.5 --> 1223.8: kind of attacker to seize the fund. Uh, I mean, seize the

Dorban asset. So
1224.5 --> 1231.9: that's risking the security for sure. Anyway, uh, to conclude my presentation. So here, what is,
1232.3 --> 1239.0: uh, after, you know, these, uh, extensive, uh, the literature review and so on, uh, what I
1239.7 --> 1245.5: thought, uh, missing in the current status is, uh, first of all, the migration requirements,
1246.0 --> 1253.0: there are no, like agreed upon migration requirements, like some, uh, study or, uh,
1253.2 --> 1258.0: defining some cryptographic requirements, like correctness, long-term integrity, and now
1258.0 --> 1262.4: first unforgivably, but I mean, this is really, this is really ideal. And there should be some
1262.4 --> 1268.0: practical requirements like, uh, security during the transition was the remedial mechanism for the
1268.0 --> 1274.7: asset. And also again, the other primitive should be other primitives, like rollout, I'm sorry.
1275.5 --> 1283.6: Uh, scaling a smart contract. I mean, those should be covered too. And like, first of all,
1283.6 --> 1287.9: I mean, before that, I mean, what's the definition of the PQC secure blockchain and what's the
1288.6 --> 1296.1: definition of the PQC migration completion, even those core, uh, definition are still quite vague
1296.6 --> 1302.7: and also the migration scope is important. Again, uh, Bitcoin quite focusing on the
1302.7 --> 1307.1: TICS transaction signature scheme migration. On the other hand, Ethereum discussion has
1307.1 --> 1314.5: been focused on the consensus layer, like BLS, BLS, my bad, sorry, BLS signature, uh, migration.
1315.2 --> 1320.5: Now, I mean, recently they kind of shifted to the, uh, execution layer too, but still,
1320.5 --> 1328.1: uh, it's kind of unbalanced yet, I guess. And, but again, what about the scale information and
1328.1 --> 1333.7: so on? Like, you know, the coverage of this migration, uh, should be also clearly defined
1333.7 --> 1341.0: before moving on to this specific discussion item. And also, uh, after that, the designing,
1341.2 --> 1347.5: you know, balance and incentive aligned migration strategy is important. Uh, as we saw, there seems
1347.5 --> 1354.8: to be no silver bullet in the blockchain PQC migration plans. It's like, it's like solving
1354.8 --> 1360.7: the game theory, you know, governance problem of motivating the majority of the stakeholders to
1360.7 --> 1367.4: participate actively in the migration. And it requires the, you know, detailed, uh, analysis
1367.4 --> 1375.8: of the stakeholder interest again. And lastly, to give the path to the next presentation or
1375.8 --> 1382.0: discussion. Well, again, I mean, because we're having the competition, we need to discuss the,
1382.1 --> 1389.7: what's the evaluation metrics, is it a total overhead or

migration speed or is there any,
1389.9 --> 1398.2: is there anything else? Okay. What, uh, yeah, let me brie fly cover this. So again, I mean,
1398.2 --> 1407.0: the Dorman method is, uh, very like interesting for me, l ike drawing my attention. And so the
1407.0 --> 1416.7: model, the PQC migration, uh, academic model is, I'm sorr y, the already proposed, uh, migration
1416.7 --> 1422.3: model is shown above, but the realistically because of th e Dorman method, uh, there should
1422.3 --> 1433.3: be the other phase where like, uh, both the legitimate ow ner of the wallet and also the
1433.3 --> 1442.5: quantum attacker, uh, try to, you know, the fund around, uh, maybe, so this model is a little more
1442.5 --> 1450.2: realistic and maybe, you know, uh, start from, you know, thinking of this migration model formally
1450.2 --> 1456.1: could be a good starting point, uh, to think about the ot her, you know, discussion items.
1456.9 --> 1460.0: And that's conclude my presentation. Thank you for listen ing.
1464.5 --> 1470.0: Thanks for sharing Keegan. That was really comprehensive. I feel like I'm
1471.1 --> 1477.0: more knowledgeable about the path that we need to take in order to get PQC. I do have a couple
1477.0 --> 1484.5: questions and then I'll obviously open up to the room, uh, for comments. Uh, a couple of things
1484.5 --> 1491.3: that will the miners need to have new hardware, um, for t his to happen was one of the questions
1491.3 --> 1498.2: that I had. And is that going to be like a cost or is tha t going to be, is it going to be a market
1498.2 --> 1507.3: that emerges because of that? Um, my second question was around like the zero knowledge proof,
1507.3 --> 1519.9: um, PQC, uh, key section and is it a mitigation if you ca n reduce the, um, like the required compute
1519.9 --> 1528.6: for a zero knowledge proof? Does that support that PQC, u m, transition if, yeah, if CKPs can
1528.6 --> 1536.2: be computed more easily or with less compute, um, does th at mean that we lean more in that direction
1536.2 --> 1545.2: versus the, uh, just retrofitting the PQC keys? All right. Rollback option. Yeah. They're my
1545.2 --> 1553.4: questions. Yeah. Thanks for asking. So talking about the, uh, miners hardware, well, I mean,
1553.4 --> 1562.4: obviously like, uh, they find the PQC signature, uh, can be done in the, like any, by any computer,
1562.8 --> 1571.3: any classical computer, but, um, I'm not very sure about the, you know, uh, the implementation
1571.3 --> 1579.1: level, uh, you know, optimal optimization of the verifica tion or signing for those PQC signature.
1581.8 --> 1589.1: But, uh, well, but talking about the profitability of, I' m sorry, I got confused between miner and
1589.1 --> 1596.3: node, but if you're talking about miner, then I mean, any

way, I'm don't really see the direction
1596.3 --> 1603.1: within the community saying like, uh, we need to change t
he structure of the hash function being
1603.1 --> 1609.8: used in the proof of work. So, um, in terms of the profit
ability of those miner, then I don't
1609.8 --> 1616.3: really see the, a lot of possibility that, you know, the
new hardware specifically designed for
1616.3 --> 1623.6: the PQC, uh, post-quantum world will emerge and making a
new market, but I might be wrong on this.
1624.4 --> 1631.4: No, that was the question. So if, so it's more important
for node operators to like upgrade.
1631.5 --> 1640.4: Well, yeah, yeah, yeah. Yeah. For enhancing the, uh, thro
ughput then, yeah, I think it's, oh.
1641.0 --> 1647.9: Uh, so on top of the Ethereum, we don't need any hardware.
 Uh, we're just only using the CPU.
1647.9 --> 1655.9: Uh, we need, uh, Poseidon too, and, uh, we're building so
me kind of XMSS signature schemes
1655.9 --> 1661.4: and verify on GKBM and GKBM on the, just only CPU.
1664.5 --> 1667.0: Yeah. Thank you for adding the detail.
1668.1 --> 1676.6: Well, actually that brings one question from my side. So,
 uh, what's the Poseidon aiming for?
1676.6 --> 1681.9: I, I got, I saw some, you know, Ethereum community news,
like Poseidon, I mean,
1681.9 --> 1688.4: the competition for Poseidon happened, right? Uh, so we,
uh, so on the Ethereum front, uh,
1689.6 --> 1696.9: on top of the consensus layer, we just bring, uh, PLS to
XMSS aggregation scheme.
1697.3 --> 1701.2: Right. And in XMSS, we're using the Poseidon too.
1702.6 --> 1704.0: Okay. I get it. Okay.
1704.0 --> 1708.4: It's specifically for XMSS. Got it. Got it. Got it. Thank
 you so much.
1710.2 --> 1717.2: So also talking about the second question from Mitchell a
bout the, uh, PQZKP, uh,
1717.4 --> 1724.0: in optimization, obviously the aggregation, uh, for, uh,
aggregation of those ZKP, uh,
1724.0 --> 1728.7: for enhancing the, you know, throughput and also the veri
fication, uh, for optimizing
1728.7 --> 1737.0: the verification cost is proposed. And I mean, even any p
roposal found in, uh, both community,
1737.1 --> 1743.5: I mean, production communities about the use of, uh, you
know, those ZKP are kind of,
1743.5 --> 1750.2: are already assuming the use of aggregation, uh, you know,
 for the performance optimization.
1750.7 --> 1752.6: Does that answer my question? Does that answer to your qu
estion?
1758.5 --> 1764.3: No, no, I answered to the Mitchell's question. Mitchell's
 second question about the
1765.4 --> 1770.5: ZKP, I mean, optimization. And so the aggregation might b
e the answer for that.
1772.4 --> 1780.0: Yeah, I think so. Um, I'm not totally sure. I just assume

that over time we're going to be
1780.0 --> 1788.5: getting better at, um, computing ZKPs and that could run in parallel with this work.
1790.9 --> 1791.4: Got it.
1808.7 --> 1812.7: Uh, do we have any other questions from the room from all four Keegan?
1815.4 --> 1816.4: Otherwise we can
1825.3 --> 1834.9: Thanks for the presentation. I have one question. You refer to the post-quantum address, uh,
1835.0 --> 1849.8: no, maybe you saw, you said that non-reused address is post-quantum. Um, maybe I think it
1849.8 --> 1864.7: depends on the expectation, like when we broadcast our transaction in MEMPU and if MEMPU takes one
1864.7 --> 1874.7: hour, quantum computer can break their, you know, exposed signature, you know, by the way. So
1875.5 --> 1884.1: maybe it's quite tiny point to discuss, but yeah, it might be possible that we can not call the
1885.6 --> 1894.0: non-reused address as a post-quantum when it comes to, yeah, there are some expectation,
1894.9 --> 1899.7: like post-quantum computer, quantum computer can break their
1902.3 --> 1911.2: public key, uh, from signature information, uh, in one hour, for example. So do you think we have
1911.2 --> 1920.1: to define the scope, like, uh, quantum computer's ability is in this scope or in that scope or
1920.1 --> 1926.7: something like that? Do you, do we have to do that? Yeah. Thanks for asking. So that point is
1926.7 --> 1933.1: actually, uh, the terminology for that point is called long-term attack and short-term attack.
1933.4 --> 1938.3: And so the long-term attack is, you know, where the quantum computer, the quantum attacker has
1938.3 --> 1946.6: enough time to, you know, run the short algorithm and get the, uh, signing key. And that is aiming
1946.6 --> 1952.9: the, you know, publicly exposed address. And the short-term attack is what you mentioned, you know,
1952.9 --> 1960.1: that attack against the mempool. So, uh, even the address is not non-reused, uh, once it's
1960.1 --> 1968.0: broadcasted to the mempool, then that's going to be, uh, the target, uh, of the, of that attack,
1968.2 --> 1974.8: that type of attack. And well, talking about this, talking about the definition of the
1974.8 --> 1982.5: post-quantum address, then I personally believe that post-quantum address should mean, uh,
1982.9 --> 1992.7: the address that, uh, the address whose, uh, public key, I'm sorry, whose verification
1992.7 --> 1999.3: can finding keys, the post-quantum signature algorithm based. That is the, maybe the
1999.3 --> 2005.1: clearest definition of the post-quantum address and whether we can say that such, you know,
2005.4 --> 2012.6: others non-reused, uh, addresses as the quantum, as the p

eak, I'm sorry, as the post-quantum address
2012.9 --> 2020.2: I'm kind of skeptical. I mean, I might think that'll be a nyway, a quantum vulnerable address
2020.2 --> 2028.6: because again, as you said, even the address, uh, is norm ally used, that's going to be, uh,
2028.6 --> 2034.3: the subject to the short-term attack by the quantum compu ter. So that's all.
2034.6 --> 2038.8: Maybe I, I understood how your presentation, I guess. Yea h. Thanks so much.
2039.6 --> 2046.6: Thank you so much. Um, so basically the post-quantum addr ess is, uh, you know,
2046.7 --> 2055.0: based on the long-term post-quantum resistant in your def inition. And we don't, so all the
2055.0 --> 2067.3: short-term attackable addresses will be classified as a n on-quantum, uh, address. Is that correct?
2068.4 --> 2076.5: Yes. Short, any address, uh, can be, that can be subject to the either short-term attack,
2076.7 --> 2084.5: long-term attack, they'll be quantum vulnerable address, non-peaky. Yeah. Yeah. That's my, yeah.
2086.0 --> 2087.4: That's how I define it.
2093.1 --> 2094.6: Any other good questions?
2105.2 --> 2105.6: Okay.
2110.1 --> 2114.9: More just, uh, I just wanted to comment that I really, um, uh, sorry, this is Carol House. Um,
2114.9 --> 2119.8: I just wanted to comment that I'm, I really, I'm glad tha t you were accounting for the issue of
2119.8 --> 2124.8: like trust in the system and impact on users. Cause I thi nk some of the different options,
2124.8 --> 2130.7: like if you have to put into a sentence, like what, what some of those decisions may mean,
2130.8 --> 2137.5: if the more centralized players in the space, like devs a nd miners end up making the decisions
2137.5 --> 2142.7: that benefit them over the users, what that will do to th e ecosystem, um, for Bitcoin specifically,
2142.7 --> 2146.8: I think this is going to be, it's, it's really interestin g. So overall, just, um, really
2146.8 --> 2151.7: fantastic overview, um, and assessment of the trade-offs. Thank you so much.
2155.7 --> 2162.1: I off that comment to do we see a world where Bitcoin is almost
2162.1 --> 2171.7: like the Guinea pig of this situation that as the, anyway, I'll just leave that one there.
2180.4 --> 2189.0: Yes. Thank you for the presentation. So please show us th e slide about the key side comparison.
2190.1 --> 2201.1: Maybe the page nine or seven. The choice of the algorithm should be decided by each committee.
2201.1 --> 2218.5: So now I'm interested in the SKU sign one, the last of th e comparison slide. So we can see that
2219.5 --> 2227.1: this algorithm has the key side and also the signature si de that is so very short.

2227.1 --> 2235.4: So it is a so big, uh, the advantage for the PQC migratio n blockchain. So, uh, but the
2235.4 --> 2241.6: opportunity that we know that the SKU, uh, SKU sign, uh, dropped out, uh, from the list competition
2241.6 --> 2249.1: at the bat, uh, SKU sign version two, uh, released. So we can see that the, uh, the choice of the,
2249.2 --> 2255.1: uh, the algorithm, uh, that should be, uh, uh, decided, u h, by the, uh, by the each committee.
2255.1 --> 2263.5: So the, uh, the choice of the, uh, choice about, uh, uh, the choice of, uh, the SKU sign is, uh,
2263.5 --> 2269.3: uh, uh, reasonable for, uh, the blockchain committee. Uh, do you think about it?
2272.9 --> 2279.0: Oh, sorry. Could you repeat the question again? So I'm ta lking about the signature side. So, uh,
2279.0 --> 2291.8: well, if I understand it correctly, well, I mean, yeah, t hough the signature employed, uh, for,
2291.9 --> 2298.9: for that specific blockchain, it's actually, you know, th e decision made by the community. Right.
2299.2 --> 2306.6: And I guess the reason, I mean, why, you know, the SKU si de sign, uh, it's not, it's not the
2306.6 --> 2312.6: option I see widely in the community is the high signing costs in this, uh, and also the
2312.6 --> 2319.1: high verification costs at the same time. So maybe the bl ockchain committee are kind of hate,
2319.2 --> 2324.8: like, uh, employing such, you know, high cost in the sign ing the verification. That's my
2324.8 --> 2334.0: understanding, but, uh, well, does that, does that answer your question? Yeah. Yeah. Yeah.
2334.0 --> 2340.6: Thank you so much. So we, we have to care about the, the, the variety, variety of that.
2341.0 --> 2342.1: Yeah. Yeah. Yeah.
2342.1 --> 2343.0: Signature algorithms.
2343.3 --> 2343.9: Yeah, for sure.
2344.1 --> 2351.7: The one, one committee, uh, uh, maybe, uh, maybe, uh, uh, maybe, uh, make the decision, uh, uh,
2351.7 --> 2360.8: to use the, this kind of the, uh, uh, uh, this kind of th e bad, bad algorithm.
2360.8 --> 2371.3: Uh, that, that means that the, uh, uh, also the, uh, NIST competition, uh, uh, uh, I think that
2371.3 --> 2377.9: the NIST competition is, uh, the, uh, uh, one of, uh, one of the choice. So that we should, should,
2378.2 --> 2387.2: should care about, and also the, uh, study, and all, all, all of the, uh, uh, all of the, uh,
2387.2 --> 2394.6: uh, signature algorithm, algorithm, uh, that have, uh, th e, uh, quantum.
2395.8 --> 2400.5: Uh, against the quantum computer. Thank you so much.
2401.0 --> 2406.7: Great, great. Thanks so much. Yeah. And actually, that's my interest too. You know, like, uh,
2407.0 --> 2412.8: for example, I see that this question, uh, maybe someone in the room can be correct me if I'm

2413.0 --> 2418.0: But I see, you know, for example, incrementing the Falcon signature
2418.0 --> 2423.8: scheme on the smart contract executable manner, then that may
2423.8 --> 2428.0: require the change of the hash function being used within this
2428.0 --> 2432.3: signing algorithm. And well, that's, that's actually, you
2432.3 --> 2435.3: know, getting away from what's defined in the NIST competition.
2435.8 --> 2440.8: So now it's like getting hard to, you know, ensure the security
2440.8 --> 2444.9: for that implementation. And well, those configuration or
2444.9 --> 2450.7: adaption will be will be made by each community too. So like,
2451.3 --> 2456.0: that's my interest to like, you know, how if in case the
2456.0 --> 2459.9: blockchain community decided to, you know, use, like some other
2459.9 --> 2463.4: signature scheme, some signature scheme other than what's being
2463.4 --> 2467.2: standardized by NIST or the other organization, then what's
2467.2 --> 2470.5: gonna be the risk assessment or how we can ensure those
2470.5 --> 2473.4: security? But anyway, thank you for the comment.
2488.5 --> 2491.0: So we move on to the competition discussion?
2492.4 --> 2496.9: I think so. There are no more questions in the room for this
2496.9 --> 2500.4: presentation. So yeah, let's move on to the next
2512.5 --> 2517.3: Hello, so I can I share that a little more detail about that
2517.3 --> 2522.2: competition itself. So good news is that we have that participant
2522.2 --> 2527.4: from NEDO here. So we have that two person from NEDO. Pretty
2527.4 --> 2531.3: quickly if I'm wrong, but so I had a much conversation with
2531.3 --> 2534.9: NEDO before the block number holding about the design of this
2534.9 --> 2538.6: competition. Then I would like to a little bit more about that
2538.6 --> 2543.5: PQC part. So as Kondo-san explained at the announcement
2543.5 --> 2548.0: session, so the purpose is providing transition technologies
2548.0 --> 2552.0: to post-condom encryption for blockchain system. So, you know,
2552.3 --> 2558.1: as Kien presented that, what is the target area? Not only that
2558.1 --> 2561.8: layer one technology, but so we need we might need to discuss
2561.8 --> 2565.5: about layer two or something like that. But it's up to that

2565.5 --> 2571.3: discussion here. But anyway, so originally, so we are mainly
2571.3 --> 2578.6: thinking on that layer one, but if it's not sufficient to cover
2578.6 --> 2583.1: that security problem caused by quantum computer, so we need to
2583.1 --> 2588.8: think about some additional area for this competition. Then, you
2588.8 --> 2594.3: know, Kondo-san already explained that background, and Kien
2594.3 --> 2601.3: already explained background, but so we will gather that, you
2601.3 --> 2601.6: know, there is some part of the competition, for example,
2601.6 --> 2605.7: migration or transition technologies, mainly on that
2605.7 --> 2610.7: layer one, but might be covered some part of the layer two or
2610.7 --> 2617.9: other part. Then the first thing is, you know, it's a, you know,
2618.1 --> 2621.0: generally for the NIST for the cryptography algorithms
2621.0 --> 2626.5: competition, for example, AES, SHA-2, SHA-3, quantum
2626.5 --> 2631.6: cryptography. So after, you know, after this decision of
2631.6 --> 2636.5: that initiating a new project, NIST holds, generally holds,
2636.7 --> 2642.0: holds that some workshop to hear that what kind of technology,
2642.1 --> 2645.4: technology specification needed before starting the competition.
2646.3 --> 2651.8: So in my experience happened 2004 and five, upon that, you
2651.8 --> 2656.3: know, the compromise of the SHA-0 and SHA-1. So they hold
2656.3 --> 2662.3: their workshop as a part of, as a, as a associated workshop,
2662.5 --> 2668.7: a crypt conference, I think in August 2020, 2005, to gather
2668.7 --> 2672.2: that what kind of that, you know, specification needed for
2672.2 --> 2681.4: the future SHA-1 and SHA-3. And then after collecting a series
2681.4 --> 2685.5: of papers to discuss about it, so NIST will create that
2685.5 --> 2689.9: specification of the competition itself. And so they
2689.9 --> 2693.6: will, they publish that specification inside other
2694.3 --> 2699.4: federal register as a, as a, you know, the information providing
2699.9 --> 2704.0: about the competition itself. Then so NIST started at the
2704.0 --> 2708.7: competition. It's a two round, three round competition. It
2708.7 --> 2713.5: takes, you know, over four and five years before deciding that
2713.5 --> 2717.1: actually the winner of the SHA-3 competition. So you know,
2717.2 --> 2721.9: general style of the NIST competition. And of course that

2721.9 --> 2725.1: this is a shorter than the, you know, the ordinary NIST
2725.1 --> 2729.7: cryptographic competition. NIST has spent five or more ye
ars
2729.7 --> 2733.0: for each competition. But unfortunately this competition
2733.0 --> 2738.2: is so three years competition. But so back to that, that
2738.2 --> 2743.4: question happened in the announcement session. So that
2743.4 --> 2747.3: what is, so what is their, you know, their call for paper
2747.3 --> 2751.2: happened this year? Is this is the purpose of the call fo
r
2751.2 --> 2755.0: paper or holding, you know, academic conference, it's a f
all
2755.0 --> 2759.5: this year in Japan, is a just kind of that, you know, the,
 you
2759.5 --> 2762.8: know, academic conference to decide the specification of
the
2762.8 --> 2767.1: competition itself, what kind of technology needed, how w
e
2767.1 --> 2771.7: evaluate it, something like that. And, you know, it's hel
d
2771.7 --> 2775.9: in one of the Japanese biggest security symposium, academ
ic
2775.9 --> 2780.4: conference symposium happening in the late October. And s
o we
2780.4 --> 2784.0: have that session, so not decided yet, but we hope to hav
e
2784.0 --> 2790.0: a half a day session about it to invite that best, great
paper to
2790.0 --> 2794.7: discuss about it. Then so after that, right after that, y
ou know,
2794.7 --> 2797.3: NEDO and the Japanese government will decide the
2797.3 --> 2801.1: specification of the competition. After that, so that
2801.1 --> 2804.0: competition, actually competition started, you know,
2804.0 --> 2808.3: each, you know, scientists, engineers, or, you know, anyo
ne
2808.3 --> 2813.3: can apply to the competition. So they have about one year
 to
2813.3 --> 2817.7: create a new technology. And they need to publish the, yo
u
2817.7 --> 2823.0: know, some papers to describe that algorithms or protocol
s on
2823.0 --> 2826.7: the transition. So they need to provide some, you know, s
oftware
2826.7 --> 2831.6: code or hardware design to realize it for the external
2831.6 --> 2838.8: evaluation. Then they need to publish some self-evaluatio
n
2838.8 --> 2843.0: document for their proposal. So that is, you know, typica
l way
2843.0 --> 2847.3: that NIST is, when NIST holds that kind of competition. A
fter
2847.3 --> 2850.9: that, so begin, you know, organize the evaluation committ

ee
2850.9 --> 2856.3: and then we will create a global test of it to evaluate a
ctual
2856.3 --> 2861.4: implementation that, that kind of thing. So it happened t
hat
2861.4 --> 2867.9: we need a lot of, a lot of fiscal year, 2027-28. Then so
2867.9 --> 2872.9: having, after having the six month evaluation period, so
we
2872.9 --> 2876.3: will decide the winner of the competition and the winner,
 the
2876.3 --> 2880.5: winner of the competition will receive, I don't know, but
2880.9 --> 2887.1: probably, you know, $200,000 or $300,000. So this is a co
mpetition
2887.1 --> 2892.2: looks like. And so during our discussion with NEDO and th
e
2892.2 --> 2896.5: Japanese government, the target blockchain technology, th
e
2896.5 --> 2900.1: Bitcoin and Ethereum, these are two major blockchain
2900.1 --> 2904.5: technologies. So, so this is the reason why that we are n
ow
2904.5 --> 2908.2: starting talking with the Ethereum Foundation person to
2908.2 --> 2912.8: have some collaboration with them. Then, of course, so we
2912.8 --> 2916.2: already reached out to the several Bitcoin Core developer
s
2916.9 --> 2922.8: for the, you know, thing. And, and I hope that, you know,
 in
2922.8 --> 2930.1: their evaluation committee, so begin, we'll organize. So,
 so I
2930.1 --> 2933.1: hope that several, you know, engineers from Ethereum
2933.1 --> 2938.2: Foundation, Bitcoin Core developers, as well as some
2938.2 --> 2942.5: experts from these other related organizations will join
that
2942.5 --> 2946.7: evaluation committee. So as Kondo-san explained that, in
2946.7 --> 2953.7: the announcement session, so generally this kind of Japan
ese
2953.7 --> 2957.7: government organized competition, the applicant is
2957.7 --> 2960.4: limited to the Japanese people or Japanese organization,
2960.7 --> 2963.8: because that prize is given to the Japanese, to that winn
er.
2964.6 --> 2970.4: But so for this competition, so as Kondo-san said, so we
would
2970.4 --> 2975.3: like to make it as much as global thing. So anyone in the
2975.3 --> 2980.8: other country than Japan can apply to that competition. T
hat
2980.8 --> 2986.1: is, that's a great thing. Then, of course, so we can incl
ude
2986.1 --> 2990.4: that, you know, the experts from all over the world for t
he
2990.4 --> 2994.5: evaluation itself. Anyway, that is an overview of that
2994.5 --> 3002.9: competition, I can say now. And, but so attendees from NA

TO, so
3002.9 --> 3007.4: is there any additional thing or is there any correction? I
3007.4 --> 3013.2: might say some wrong thing. Is that okay? Okay. Great. Thank
3013.2 --> 3016.8: you. So this is explanation of that competition, how the
3016.8 --> 3021.8: competition looks like as a whole. Is there any question
3021.8 --> 3024.9: about that, that organization? Of course, are you, so we will
3024.9 --> 3030.1: discuss by utilizing the last 40 minutes, so we will discuss the
3030.1 --> 3033.8: detail about that technology. But before that, so is there any
3033.8 --> 3036.2: question about that, the competition design?
3038.0 --> 3043.9: I've got a question about the evaluation committee. Is there
3043.9 --> 3048.7: like, what is the proposed governance for the evaluation
3049.3 --> 3057.9: committee? Is it more, these are the experts and I'm just kind
3057.9 --> 3061.1: of thinking forward in a year's time when we have a whole bunch
3061.1 --> 3067.1: of really, really brilliant projects that are applying for
3067.1 --> 3072.8: the competition. How do we ensure that they feel like it's
3072.8 --> 3077.2: a fair competition based on their perspective of the
3077.2 --> 3082.5: evaluation committee? And what the timeline is, is kind of
3082.5 --> 3084.3: what's coming to mind for that?
3085.1 --> 3088.7: Okay, so this is my understanding, what NIST is
3088.7 --> 3094.0: doing for this type of competition. So for the NIST
3094.0 --> 3098.6: competition, I might be, I might say wrong thing, but so for
3098.6 --> 3103.7: NIST competition, the organization who decides the
3103.7 --> 3108.2: winner is NIST. But, but so they have the very, you know,
3108.3 --> 3112.5: neutral academic process to decide it. They hold their, you
3112.5 --> 3118.5: know, workshop one or two times every year to discuss about the
3118.5 --> 3123.1: process. And the cryptographers all over the world participate
3123.1 --> 3127.8: to that workshop and any evaluation process. It's a very
3127.8 --> 3132.7: transparent process. The transparency for the, to that,
3132.8 --> 3137.8: that cryptographer all over the world is a source of the, you
3137.8 --> 3143.7: know, credibility of the process itself. And, you know, I would
3143.7 --> 3146.8: like to copy and paste that kind of style. So, you know, begin
3146.8 --> 3149.9: organize that kind of the transparent series of workshop

3150.6 --> 3152.8: to make it more legitimate.
3156.1 --> 3158.8: I don't know. I don't know. So.
3161.1 --> 3164.1: Andy, I see that you're online. If you're still there, di
dn't
3164.1 --> 3169.2: know if you wanted to comment on thoughts or, or just rea
lize
3169.2 --> 3172.6: not in shaping this one necessarily, but on the kind of
3172.6 --> 3176.1: criteria that NIST has used historically on competition s
ort
3176.1 --> 3178.8: of like this, where they were looking for innovative solu
tions
3178.8 --> 3180.6: and, and evaluating them.
3182.0 --> 3186.6: Yeah. And I, I think the description that we heard a
3186.6 --> 3189.7: moment ago, I think that's fairly accurate to how we've,
3189.9 --> 3193.3: we've operated when we've done competitions. I, I will sa
y, I
3193.3 --> 3198.1: think it's very important to, throughout the process to s
ort
3198.1 --> 3202.4: of keep everyone on the same page about what the goals an
d
3202.4 --> 3207.0: the evaluation criteria are basically, you know, how, how
3207.0 --> 3210.1: you scope it and how you set those initial security
3210.1 --> 3215.9: requirements and evaluation criteria is, is critical to
3215.9 --> 3223.1: having buy-in throughout the process. Continuing to get,
you
3223.1 --> 3226.4: know, feedback from the community through, through the,
3226.7 --> 3230.1: through the process is also critical. But then also, you
3230.1 --> 3233.3: know, ultimately explaining the decisions, you know, in
3233.3 --> 3239.3: addition to those workshops that we hold to have, you kno
w, to
3239.3 --> 3242.5: to hear feedback on the, you know, on the candidates, we
3242.5 --> 3245.6: also then, you know, when it is time to make a decision a
nd
3245.6 --> 3251.3: make a selection, we write reports that go through, you
3251.3 --> 3254.7: know, our understanding of the candidates and how we eval
uated
3254.7 --> 3259.2: them and how we got to the selections that we did. I thin
k
3259.2 --> 3264.6: that's another important part to, to transparency. You kn
ow,
3264.6 --> 3270.8: obviously with, you know, the, the broader the effort, I
think
3270.8 --> 3275.6: some of the, can be more challenging in terms of scope.
3275.7 --> 3278.7: And so I think, you know, some of those initial discussio
ns
3278.7 --> 3284.6: that this group has around how to, you know, how to defin
e
3284.6 --> 3288.6: things or how to lay it out is going to be important to t
he,
3288.7 --> 3290.5: the success of the project longer term.

3292.9 --> 3296.0: When NIST has run them before, do you, I don't know if yo
u
3296.0 --> 3300.1: recall, and this may not be fair for you if I'm not sure
how
3300.1 --> 3303.8: many of them you've done directly. Were NIST, was NIST
3303.8 --> 3307.6: normally looking at evaluation criteria of the technology,
 or
3307.6 --> 3311.2: did it normally bridge into like impact, but also busines
s
3311.2 --> 3315.7: viability, the way that like a VC, like or others may ass
ess
3315.7 --> 3319.9: solutions, just curious, like, I don't know, as there's,
as, you
3319.9 --> 3322.6: know, Nito is thinking about how to assess it. I'm just
3322.6 --> 3325.2: curious, like what NIST has turned to? Was it, was it
3325.2 --> 3328.8: normally just focused on tech? Or was it also focused on
like
3328.8 --> 3329.7: business viability?
3330.8 --> 3334.6: I mean, it's really been very technically focused for the
3334.6 --> 3337.7: underlying component. So that looks, you know, would look
 at,
3338.1 --> 3341.9: you know, the, the security analysis of the, the scheme,
3342.0 --> 3347.4: including kind of how well understood it is and mature, y
ou
3347.4 --> 3350.7: know, would also look at suitability, but suitability in
3350.7 --> 3354.8: the context of a cryptographic algorithm means looking at
 the,
3355.4 --> 3359.3: mainly at the performance characteristics. And as part of
3359.3 --> 3364.2: that, you might look at, you know, consider different use
3364.2 --> 3367.4: cases for a particular algorithm in different, different
3367.4 --> 3370.5: environments. But I think that's probably, you know,
3370.5 --> 3373.9: fundamentally a different, you know, level than, you know,
3373.9 --> 3377.6: maybe, let's say, business viability at a, at a system
3377.6 --> 3378.0: level.
3381.4 --> 3386.3: Thank you very much. So I agree with you that because tha
t all
3386.3 --> 3391.8: parts, this competition is about the cryptographic primit
ives.
3393.0 --> 3396.0: But this competition on the cryptographic protocols relat
ed
3396.0 --> 3399.8: to that very, some business model or something like that.
 So
3399.8 --> 3404.7: that is a huge difference between the existing competitio
n
3404.7 --> 3409.0: and this, you know, competition for the blockchain, you k
now,
3409.1 --> 3413.6: PQC migration for a specific industry, a specific use cas
e
3413.6 --> 3414.3: is like a blockchain.
3416.9 --> 3420.6: And the result, so without knowledge about that actual us

e
3420.6 --> 3423.8: case, actual business model of the blockchain, as Keegan,
 you
3423.8 --> 3428.1: know, Keegan's presentation, so illustrate it a lot about,
 you
3428.1 --> 3432.0: know, without, you know, discussion about that, how the
3432.0 --> 3437.1: stakeholders in the blockchain world acts or habits, no o
ne
3437.1 --> 3441.2: applied to that transition plan to their, their blockchai
n
3441.2 --> 3445.8: technology. So this is a huge difference against the exis
ting
3445.8 --> 3448.0: NIST cryptographic competition.
3451.3 --> 3454.2: Is there any question about that? Okay.
3464.5 --> 3469.2: So, I'm Shoki from Nix Foundation, and I'm building new
3469.2 --> 3472.9: generation, is I am client which support post quantum tra
nsition.
3474.0 --> 3482.6: Let's talking about Ethereum. So, so in Ethereum, we have
 two
3482.6 --> 3487.8: signature scheme. One is the ECDC for end users and BLS f
or
3487.8 --> 3492.9: validators. On the consensus client we use in the BLS, wh
ich
3492.9 --> 3500.5: is already specified to migrate into XMSS. Each client al
ready
3500.5 --> 3505.1: building, keep building right now. So I guess these two g
oal
3505.1 --> 3509.0: has accomplished in consensus layer already accomplished.
3509.8 --> 3516.5: However, we don't have any specification for end user. So
3516.5 --> 3522.9: in this competition, we aim for the just end user, right?
 Is it
3522.9 --> 3523.2: correct?
3525.0 --> 3529.1: Yeah, so this is a, this is a, you know, what I would lik
e to
3529.1 --> 3532.4: discuss today. Okay, about that competition, because, you
 know,
3534.5 --> 3541.2: so what should be evaluated? Yeah. And it depends on the
3541.2 --> 3544.4: blockchain, you know, the discussion might be slightly
3544.4 --> 3547.7: different among, you know, different, among the different
3547.7 --> 3550.8: blockchain technology like Bitcoin, Ethereum or other, ot
her
3550.8 --> 3554.5: layer on technologies. And, you know, this is the purpose
 of
3554.5 --> 3557.1: this, this discussion that I would like to hear that opin
ion
3557.1 --> 3560.2: from the Ethereum engineers. So what is it? What is the i
ssue
3560.2 --> 3561.1: for Ethereum blockchain?
3562.2 --> 3563.5: Thank you. That's right.
3567.8 --> 3572.7: So is there any criteria to decide the scope right now? I

t's
3572.7 --> 3576.5: kind of scope of scope is maybe might be a bit stupid que
stion,
3576.9 --> 3584.4: but I, for example, one thing we need to be afraid of is
like,
3584.6 --> 3589.6: no, there's a so limited number of participants and we sh
ould
3589.6 --> 3596.8: give a no wise to our no, no, not appropriate idea or
3596.8 --> 3603.2: implementation. So this is not so good. So to avoid that
we
3603.2 --> 3610.9: need a quite clear criteria, clear goal and scope, which
is
3610.9 --> 3616.1: targeting the large number of people, for example, you kn
ow,
3618.1 --> 3623.5: as he mentioned before, it's signature scheme, it's very,
3623.5 --> 3631.9: very limited scope. For example, the key signature scheme
 for
3631.9 --> 3638.3: post quantum blockchain, it's quite clear somehow on the
we
3638.3 --> 3641.5: can expect that many, many participants in that because
3641.5 --> 3647.2: their scope is clear. Also, there are many people buildin
g
3648.0 --> 3652.6: post quantum signature. So yeah, it's another reason why
we can
3652.6 --> 3658.2: expect more people. On the other hand, so the best post q
uantum
3658.2 --> 3663.1: blockchain system, it's a bit wider scope and people can
not
3663.1 --> 3668.4: expect on what is criteria. People cannot have enough
3668.4 --> 3673.1: confidence to to participate their competition. Yeah, lik
e
3673.1 --> 3680.7: the way we need our kind of criteria to set a scope. And
in
3680.7 --> 3688.1: my opinion, one criteria like KPI to set a scope is numbe
r of
3688.1 --> 3695.4: the target. Yeah, for example, signature scheme, inventor,
 we
3695.4 --> 3700.5: can expect no right now 1000 people working for that in t
his
3700.5 --> 3706.8: world. Or Yeah, no, we can sit scope like the way. What d
o you
3706.8 --> 3711.5: guys think about the criteria to set the scope right now?
3712.0 --> 3714.4: Okay, thank you very much. That is the thing that you kno
w, that
3714.4 --> 3719.1: is a so what discuss with NIST person, you know, generall
y
3719.1 --> 3725.0: NIST holds the first workshop to decide scope and evaluat
ion
3725.0 --> 3731.0: criteria. Just it. So and this is the purpose of that the
3731.0 --> 3735.0: workshop held in Japan this October. So we will call for

3735.0 --> 3740.5: papers to hear opinion on that. What is the scope of the
3740.5 --> 3744.3: competition? What kind of evaluation we should do? So thi
s
3744.3 --> 3747.3: is a so what is a call for paper and that's what we discu
ss in
3747.3 --> 3752.2: the hall. Today that's pretty preliminary discussion abou
t we
3752.2 --> 3756.1: need to make a call for paper for the October workshop. A
nd so
3756.1 --> 3759.9: we need to restart that, you know, potential scope of tha
t
3759.9 --> 3763.0: workshop. And I would like to hear that opinion from from
 all
3763.0 --> 3767.4: of you to as a preliminary work to to restart it. Of cour
se,
3767.5 --> 3771.5: it's not limited to that what we discussed today. But we
will
3771.5 --> 3774.6: decide the scope, a concrete scope and the evaluation
3774.6 --> 3780.7: criteria this fall at the workshop. But this is a clear
3780.7 --> 3786.4: process. And what so NIST has been done so far for severa
l
3787.1 --> 3789.5: their cryptographic primitive competition.
3797.7 --> 3801.8: So I would go back to the key key and so if you are still
 here,
3802.7 --> 3807.7: so do you have any opinion that so what should be that sc
ope of
3807.7 --> 3808.4: the competition?
3810.6 --> 3815.4: Well, well, just just for clarification. So in the
3815.4 --> 3820.5: workshop held in October something we are discussing, I
3820.5 --> 3824.1: mean, we are calling for a paper discussing the scope of
the
3824.8 --> 3830.1: scope of the competition or like a specific idea for the
as a
3830.1 --> 3832.3: proposal? I mean, so
3832.9 --> 3840.0: that is a good question. So basically, so firstly, so we
3840.0 --> 3845.7: need to decide the scope and evaluation criteria first. O
f
3845.7 --> 3849.4: course, so we could have that some session about that. So
 the
3849.4 --> 3853.8: actual transition mechanism itself. But before that, so w
e
3853.8 --> 3857.5: need to concentrate on that scope and the evaluation
3857.5 --> 3858.2: criteria first.
3860.2 --> 3866.1: Okay. Got it. Then we're talking about the scope of the
3867.2 --> 3871.2: competition. Well, as you say, maybe the last session, it
's
3871.2 --> 3877.2: going to focus on Bitcoin and Ethereum, then, well, that,
 you
3877.2 --> 3880.9: know, like, as I say, like some scaling solutions, smart
3880.9 --> 3884.9: contract, I mean, that's, that's really domain specific.

But if we
3884.9 --> 3889.5: can narrow down enough to Bitcoin and Ethereum, then I
3889.5 --> 3891.8: don't know, wait, I don't know. I'm not very sure if that
's
3891.8 --> 3896.9: enough. But if it's, let's say, if it's Bitcoin, then I m
ean, we
3896.9 --> 3901.5: can actually list up the core primitives, or also like, y
ou
3901.5 --> 3904.6: know, maybe make some the list of the priority of those
3905.1 --> 3907.8: components are primitive primitives used in Bitcoin
3907.8 --> 3915.4: protocol. I mean, for example, this is a number of priori
ty for
3915.4 --> 3919.1: sure. But I mean, hashtag low contract, and I was like,
3919.1 --> 3922.7: hash function for POW. I mean, even the security security
 level
3922.7 --> 3925.9: for the hash function is supposed to be getting lower in
3925.9 --> 3929.3: the quantum world. So maybe that will be in the list too.
 And
3929.3 --> 3933.1: making first, first, making those lists, you know, with s
ome
3933.1 --> 3940.8: priority, and like, maybe having two or three top up, top
 up the
3940.8 --> 3945.3: list will be the appropriate way will be, it's kind of lo
ok
3945.3 --> 3951.0: appropriate way to proceed for me, you know, do you know
what I
3951.0 --> 3952.9: do get what I mean? I mean,
3954.4 --> 3960.8: I have one comment that, you know, in addition scope, so,
 so
3960.8 --> 3965.8: it was indicated in the your presentation. But so we need
 to
3965.8 --> 3973.5: discuss that the definition of the PKG ready blockchain,
you
3973.5 --> 3978.6: know, so what is the qualification about that? So we
3978.6 --> 3983.8: completed the PQC migration for so new, new blockchains o
f PQC
3983.8 --> 3987.4: ready, or something like that. So we need to discuss abou
t that
3987.4 --> 3993.1: that goal. So actual goal of that. So what so the to the
3993.1 --> 3999.2: completion, you know, I think that that that kind of
3999.2 --> 4004.8: discussion is not occurred for for other area of the PQC
4004.8 --> 4008.8: migration, as well. But for this competition, we need to
have
4008.8 --> 4013.2: some goal for the completion.
4019.6 --> 4024.0: Will the scope comes first before the goal or the goal
4024.0 --> 4029.1: comes up before the scope defining scope? So, because,
4029.5 --> 4034.4: well, if you want the perfect, I don't know, I don't even
 know
4034.4 --> 4039.3: like what the quantum secure means. But if, obviously, we
 can

4039.3 --> 4043.6: list up every every tech stack, you know, on the protocol, or
4043.6 --> 4046.8: they know execution of the Bitcoin, I mean, etherium
4046.8 --> 4052.8: software, and like, and any risk can be found, I guess, because
4052.8 --> 4059.5: even the hash function may be risk. And if we try to define
4059.5 --> 4063.3: the goal before narrowing down the scope, then that goal will
4063.3 --> 4069.6: be very, you know, how to how to stick explosively big. And if we
4069.6 --> 4072.8: actually if you try to formally define the goal, then I don't
4072.8 --> 4077.7: know, we can handle it. So I understand, I thought the scope
4077.7 --> 4084.1: comes first and the maybe goal will be defined for each. Is
4084.1 --> 4085.0: that the way to proceed?
4090.2 --> 4096.1: Well, I think you probably have goals at different levels,
4096.4 --> 4099.4: there's sort of the overarching kind of goal that you're trying
4099.4 --> 4103.0: to achieve. And then, you know, there's the once you set the
4103.0 --> 4106.6: scope, the more specific objectives that that you're
4106.6 --> 4110.4: trying to do within that scope. You know, again, this is this
4110.4 --> 4113.5: isn't really something that we've had to deal with with the
4113.5 --> 4116.1: NIST competitions as much because we were focused on
4116.1 --> 4118.7: individual components. But I think, yeah, when you're looking
4118.7 --> 4122.5: at a broader system, that's going to be more challenging to
4122.5 --> 4126.7: parse out into, you know, into the different levels.
4128.3 --> 4128.8: Right.
4131.4 --> 4137.5: Can I speak a bit? So to elaborate their imagination about
4137.5 --> 4142.6: this are this competition, I want to do some kind of
4142.6 --> 4148.8: brainstorming, like, for example, yeah, you said that post
4148.8 --> 4155.5: quantum migration. So the scope will be limited to Bitcoin or
4155.5 --> 4160.4: Ethereum, you said, maybe it's appropriately kind of narrow
4160.4 --> 4166.7: scope. So to elaborate their further imagination, so if you
4166.7 --> 4170.9: take our Bitcoin, for example, so we need to, yeah, the
4171.4 --> 4175.4: competition will be on post quantum migration of Bitcoin.
4175.4 --> 4186.7: And, and the last presentation, you are shows or how to the

4186.7 --> 4192.7: migrate, say the migrate period, the governance of their post
4192.7 --> 4199.9: quantum migration. So it's a scope about their governance, or
4200.7 --> 4205.7: the participant should also submit their, you know,
4205.9 --> 4211.6: signature scheme about the post quantum competition, or
4211.6 --> 4217.4: participant can only know, they can only submit their governance
4217.4 --> 4222.7: system without that perspective. Yeah, so something like that. So
4222.7 --> 4228.6: maybe the governance, so we need to know, cut into their pieces,
4229.2 --> 4235.6: like governance, and scheme, and primitives, and then we can sit
4235.6 --> 4240.1: there, no set up the scope, which participants should care
4240.1 --> 4247.0: about them, but participants can feel safe to to kind of have
4247.0 --> 4248.5: their imagination about this.
4252.3 --> 4257.7: Right. Is anyone holding the mic in the room? If I have, if I
4257.7 --> 4261.6: can add some comment? Well, what? Thank you for bringing up
4261.6 --> 4266.7: the governance aspect of this conversation. But I think the
4266.7 --> 4269.8: most difficult thing is, like, it's really, it's kind of hard
4269.8 --> 4272.0: to, you know, completely distinguish the technical
4272.0 --> 4274.7: aspect of the migration plan and the governance aspect of the
4274.7 --> 4278.9: migration plan. So for example, like, in Bitcoin, there's a
4278.9 --> 4283.6: model called hourglass is proposed. So that's allowing the
4284.1 --> 4290.5: ECBSA based transaction acceptable, one transaction per
4290.5 --> 4294.2: block, even after a two day, so that, you know, those dormant
4294.2 --> 4296.8: asset holder may still have some chance to, you know, move around
4296.8 --> 4299.4: the found after a QA happens, or, you know, after they cut off
4299.4 --> 4303.9: the migration period. And they're saying that's, I would
4303.9 --> 4310.4: say, like, incentive aligned, like for even for miners. And so
4310.4 --> 4316.8: that they're saying that that's the ultimate, not the ultimate,
4317.0 --> 4319.8: maybe that's too much, but like, that's the balanced solution.
4320.0 --> 4322.7: That's their what that's what they're claiming. And, well,
4323.4 --> 4328.8: even on that systematic level, decision, like, you know,

how
4328.8 --> 4331.6: many blocks will be how many transactions will be include
d
4331.6 --> 4335.8: per block after a QA, that kind of decision will end up i
n the,
4335.8 --> 4340.4: you know, how the bidding war will be formed. And I don't
 end
4340.4 --> 4347.8: up to the governance, you know, discussion. So like, if w
e try
4347.8 --> 4353.7: to the whole poster competition talking about the migrati
on plan,
4354.4 --> 4358.6: or migration scheme, then that will necessarily include t
he
4358.6 --> 4360.1: governance aspect in the end.
4363.3 --> 4368.5: So that's my comment, I want to make, I want to confirm t
hat. So
4368.5 --> 4373.5: basically, you're thinking about the migration plan compe
tition.
4374.1 --> 4378.2: So, for example, I'm a participant, I want to come up
4378.2 --> 4385.8: with very, very good quantum, post quantum signature sche
me. I
4385.8 --> 4390.1: want to bring that idea to here, but I cannot participate
 in the
4390.1 --> 4393.6: debate because the main theme is governance. Is that corr
ect?
4393.7 --> 4394.1: For example,
4395.8 --> 4401.5: I don't think the main thing is the governance. But if th
e if
4401.5 --> 4406.2: the governance, yeah, I mean, if the Yeah, I mean, the
4406.2 --> 4412.0: operational, like, I mean, acceptability comes to one mat
ch
4412.0 --> 4417.1: metric in the, you know, for evaluating the migration sch
eme,
4417.2 --> 4418.5: then there'll be
4419.2 --> 4419.4: Yeah.
4420.4 --> 4421.4: What's happening?
4423.0 --> 4427.1: It's a technology competition. Okay, so you should propos
e
4427.1 --> 4431.9: technology itself. But so so, you know, but that technolo
gy is,
4432.2 --> 4435.6: you know, you know, operationally infeasible, or,
4435.7 --> 4442.6: you know, incentive, incentive, incentive point of view,
it's
4442.6 --> 4443.8: not feasible to implement.
4444.5 --> 4450.0: Okay, so, for example, I have a good idea of quantum, pos
t
4450.0 --> 4455.9: quantum signature scheme. Is he's a target? Is he's a kin
d of
4455.9 --> 4457.5: scope or participant?
4458.2 --> 4462.3: That is another discussion, you know, so I already have t

hat
4462.3 --> 4466.5: this tons of discussion with NATO and Japanese government about
4466.5 --> 4471.6: it. Because we already have that, you know, NIST already has
4472.1 --> 4478.1: the standard post quantum signature scheme. So should we
4478.1 --> 4482.7: reinvent the wheel to do the same thing to create that?
4482.9 --> 4488.1: I'm getting your point. And so what I want to say, try to say
4488.1 --> 4493.2: is, I think that people here still don't have our
4493.2 --> 4498.2: imagination. What is the kind of, you know, scope of the
4498.2 --> 4502.9: participant? And what kind of people can know? What kind idea
4502.9 --> 4509.0: people need to bring to this competition? And so, yeah, f or
4509.0 --> 4515.6: example, I have another idea, post quantum migration, whi ch is
4515.6 --> 4519.8: very good for Ethereum, but I don't have any idea about p ost
4519.8 --> 4524.5: quantum signature. Can I be a participant? Maybe? I don't
4524.5 --> 4528.8: think that people here still have our idea. I can be the
4528.8 --> 4530.4: participant or not, for example.
4530.7 --> 4536.3: So, you know, creating a new signature scheme is out of s cope.
4537.3 --> 4540.3: Because we already have that, you know, after seven years,
4540.4 --> 4544.5: after 80 years, NIST has tons of growth, global cryptogra phers
4544.5 --> 4549.2: tons of effort to decide post quantum signature scheme
4549.2 --> 4555.3: certified by NIST, or global, global cryptographers. That 's
4555.3 --> 4559.9: excellent. So we don't have to reinvent the wheel. So ass uming
4559.9 --> 4564.7: the existence of good post quantum signature scheme, how we
4564.7 --> 4569.0: implement or incorporate that signature scheme easily to
4569.0 --> 4572.6: blockchain system? That is the question, technology quest ion.
4579.2 --> 4583.1: The question I have is, is it about the procedure of the
4583.1 --> 4587.3: incorporation of the PQC signature into blockchain or the
4587.3 --> 4592.9: result or outcoming? I mean, I guess it's a process. It's about
4592.9 --> 4593.4: the process.
4593.7 --> 4599.0: The procedure means that business protocol itself,
4599.2 --> 4603.1: because you got that we need to write up some software or some
4603.1 --> 4607.9: system to achieve the goal from technology point of view. And
4607.9 --> 4611.7: the procedure means that, you know, some, it might be, yo u
4611.7 --> 4617.4: know, we might design some, you know, actual, you know, p

rocess
4617.4 --> 4621.1: or procedure, you know, from governance point of view, bu
t
4621.1 --> 4625.2: it's not mainstream, but so we need to, we need to think
about
4625.2 --> 4630.7: it, but it is a technology competition. So the proposing
a
4630.7 --> 4634.9: new protocol or proposing a new software is the main, you
 know,
4635.0 --> 4636.7: main part of this competition, I think.
4639.4 --> 4646.6: So I've got a question around the degrees of effectivenes
s of
4646.6 --> 4651.5: the PQC, because I assume like there's always trade offs
in any
4651.5 --> 4655.5: system. And I assume that there are going to be PQC signa
tures
4656.2 --> 4659.8: and schemes that are easier to implement, but not as long
 term
4659.8 --> 4666.1: viable, vice versa. I don't really know enough about the
PQC
4666.1 --> 4670.0: signatures to work that out. But I think that's something
 that we
4670.0 --> 4672.9: need to consider in the scope of the competition, because
 there
4672.9 --> 4678.6: might be really good short term solutions that help mitig
ate the
4678.6 --> 4683.1: risk and the problems that are inevitably going to occur
in a
4683.1 --> 4689.4: few years. But and we should reward people for proposing
4689.4 --> 4694.5: those. But that may not be a long term solution. And some
one
4694.5 --> 4697.8: may come to the competition and have a long term solution
 in
4697.8 --> 4704.2: mind that takes more degrees of, of work and something th
at we
4704.2 --> 4709.2: have to consider over a period of time, and it may be mor
e
4709.2 --> 4714.0: difficult to implement. So how do we work out the degree
of which
4714.0 --> 4718.9: it needs to be effective, I guess.
4724.5 --> 4726.5: Maybe that's just a question for the scope.
4733.1 --> 4739.3: I think that brings up, is this specifically focusing on
the PQC
4739.3 --> 4743.5: or for blockchain or is this for cryptogility for blockch
ain?
4746.3 --> 4753.2: Will the protocol, you know, cover not only for PQC, but
also
4753.2 --> 4758.7: for like, maybe some potential next signature scheme migr
ation
4758.7 --> 4760.8: happening in 30 or 50?

4761.4 --> 4766.6: Yeah, that's kind of what I'm thinking is that if the
4766.6 --> 4770.2: assumption is that this is always going to accelerate and
 quantum
4770.2 --> 4773.5: computers are always going to get better, then we should
build a
4773.5 --> 4778.7: template that this becomes sustainable. And based on what
4778.7 --> 4784.1: I've heard from the NIST, I think we did this in 05 for t
he
4784.1 --> 4789.6: SHA, and we're here 20 years later with a new threat. I t
hink
4789.6 --> 4794.6: we could assume in 20 years time, there'll either be a
4794.6 --> 4797.3: stronger quantum threat or there'll be something all new
4797.3 --> 4804.7: altogether. Perhaps we should consider that in the scope
of the
4804.7 --> 4808.3: competition and how we socialise it as well.
4808.6 --> 4814.1: Okay, on the difference between the PQC migration and the
4814.1 --> 4819.2: cryptogility, so Ito-san might have some other idea, but,
 you
4819.2 --> 4824.6: know, designing and implementing cryptogility mechanism f
or some
4824.6 --> 4830.1: specific protocol is one of the means to achieve the goal
 of the
4830.1 --> 4838.3: PQC readiness. Cryptographic agility is not a new concept,
4838.5 --> 4844.2: it's a 10 years, 20 years old concept. But it's not easy
to
4844.2 --> 4849.8: define the crypto agile for some specific protocol. But o
f
4849.8 --> 4856.4: course, if we can completely design what the crypto agile
 for
4856.4 --> 4864.4: the blockchain is easily, that is a huge win. So if we as
sume
4864.4 --> 4867.8: the goal of this competition is achieving crypto agile or
4867.8 --> 4871.3: crypto agility for the blockchain, so the problem might
4871.3 --> 4874.8: be harder than the achieving PQC readiness, I think.
4876.1 --> 4881.4: Hi, thinking about the crypto agility, I'm a bit thinking
4881.4 --> 4885.9: about a broader discussion about policy and the mechanism
4885.9 --> 4891.1: things. So, like, I think we are trying to make mechanism,
 but
4891.1 --> 4896.1: as some, like Keegan said, like, some mechanism support v
arious
4896.1 --> 4900.0: policy, for example, like, how many ECDSA signature like
they
4900.0 --> 4903.2: accept for one block or something. And there are like
4903.2 --> 4908.2: some protocol accept many variety of like policies, but
4908.2 --> 4914.1: some of them are not. So and so maybe some protocol suppo
rt
4914.1 --> 4919.8: very agile, like, crypto agile migration, but some of the
m are
4919.8 --> 4926.0: not. So not that agile. So I'm thinking like, what will b
e the

4926.0 --> 4931.3: like outer edge of the scope of change of the policy things. So
4932.0 --> 4939.0: so some, like, I think we like for some protocol, proposing
4939.0 --> 4944.0: protocol, we might need to require some policy, for
4944.0 --> 4947.7: example, like use of PQC signature or something, but
4947.7 --> 4953.6: like, for other protocol, for many candidates, they may
4953.6 --> 4959.1: support very different policy, like, some, like, for extreme
4959.1 --> 4964.1: lines, like some policy, like mechanism only support for, like
4964.1 --> 4967.4: Bitcoin, some people, like protocol only support for
4967.4 --> 4974.0: Ethereum, but, like, it might be, like, nice to think about,
4974.1 --> 4980.3: like, what kind of the range of the policy we are ready to,
4980.8 --> 4985.2: like, not support, but accept for competition. Otherwise,
4985.4 --> 4990.4: like, it's, like, very, it will be very difficult. And thinking
4990.4 --> 4997.3: about, like, functionality of the protocol, and the policy of
4997.3 --> 5002.6: the protocol is different. So think about those differences.
5003.1 --> 5009.0: Yeah. So, yeah, so I think, like, those crypto agility is
5009.0 --> 5015.7: the one evaluation, like, element, but, like, we might
5015.7 --> 5021.8: need to think about other, like, policy-related, like, element
5021.8 --> 5022.4: here.
5043.5 --> 5050.4: Just one proposal. How about doing this? So we do the
5050.4 --> 5057.5: competition among us. Maybe it's more easy than before. We
5057.5 --> 5062.7: can use LLMs and whatever we can come up with to make a proposal.
5063.4 --> 5069.8: Maybe it doesn't take one day or half day, I guess. Then many
5069.8 --> 5075.6: people make a proposal, and they make their, you know, winner
5075.6 --> 5080.9: among them. Then we can see their, what kind of criteria on
5080.9 --> 5087.7: the range of scope and policy we need to address. And, yeah,
5087.8 --> 5093.8: maybe various type of, I think that more various type of
5093.8 --> 5099.4: proposal will come from many people and, you know, than one
5099.4 --> 5103.8: person expect. And this is, you know, yeah, to make a
5103.8 --> 5109.1: competition, maybe we can make a pre-competition before that to
5109.1 --> 5114.8: demonstrate, and then we don't fail to make the range of the
5114.8 --> 5115.4: policy.

5120.3 --> 5126.5: But it should be a part of the discussion item on the sym
posium
5126.5 --> 5128.1: happening this October.
5139.0 --> 5144.1: So in terms of socializing the call for papers, we've sta
rted
5144.1 --> 5145.6: that right now already?
5146.5 --> 5150.1: Not yet, not yet. So I need to talk with Suga-san. He's t
here.
5150.8 --> 5155.7: But he's one of the organizers of that, you know, the sym
posium
5155.7 --> 5160.3: happening in October. We need to discuss with him about w
hat we
5160.3 --> 5162.8: started that call for papers, something like that.
5167.7 --> 5170.6: Yes, do you want to say something about that?
5176.5 --> 5181.8: Thank you for the introduction of me. So I'm Yuji, one of
 the
5181.8 --> 5186.8: organizers of the Domestika conference about the blockcha
in
5186.8 --> 5194.8: technology. So maybe the last week of October this year,
so
5194.8 --> 5202.2: the BWS blockchain workshop will be held at Shizuoka pref
ecture,
5202.9 --> 5212.6: maybe the Hamamachi. So we have the five days symposium a
bout
5212.6 --> 5217.6: all of the layers of information security, including the
5217.6 --> 5223.9: cryptography. And also maybe one or two days on the works
hop
5223.9 --> 5231.9: about the blockchain technology so that we can, at the fi
rst
5231.9 --> 5240.9: step, we have to write down the call for paper about this
 kind
5240.9 --> 5252.3: of competition criteria. And also we will discuss by the
5252.3 --> 5258.6: Japanese and also the English. So the published call for
paper
5258.6 --> 5265.7: will be written down in Japanese and English. So please s
ubmit
5265.7 --> 5275.8: the paper. Maybe the first week of the August call for pa
per is
5275.8 --> 5283.9: published and also the deadline of the papers will be the
 third
5283.9 --> 5292.0: or fourth week of August. Please join us. Thank you so mu
ch.
5293.7 --> 5299.3: But so we, I think that before the August, so we can do s
ome
5301.4 --> 5309.1: preliminary notification or something. And so I think we
are
5309.1 --> 5312.7: running out of time, but I would like to talk about that
test a
5312.7 --> 5316.5: bit. Because, you know, so as we discussed with Japanese
5316.5 --> 5320.4: government in the beginning, we will create that global t

est a
5320.4 --> 5325.6: bit to do some implemented evaluation on the transition o
f
5325.6 --> 5330.6: the blockchain data. And we are not thinking that so we,
you
5330.6 --> 5335.7: know, Japanese government or NATO will provide some amoun
t of
5335.7 --> 5340.2: money to begin and begin will collaborate with global
5340.2 --> 5345.0: universities to operate that test a bit node. So for exam
ple,
5345.2 --> 5348.6: you know, eight or 10 or more, I don't know how many. So
I need
5348.6 --> 5355.3: to know that how many test a bit is needed, how many node
s we
5355.3 --> 5359.4: need to do that kind of evaluation, fair evaluation. And
5359.4 --> 5363.4: if, you know, but due to that, you know, budget limitatio
n, I
5363.4 --> 5366.9: think, you know, by utilizing the Japanese government bud
get,
5367.1 --> 5371.4: we can set up that, you know, evaluation node, 10 evaluat
ion
5371.4 --> 5378.5: nodes for six months, for example. So if we can call for
5378.6 --> 5381.2: additional evaluation nodes, we can increase the number o
f
5381.2 --> 5384.9: nodes. For example, that, you know, three in Japan, you k
now,
5384.9 --> 5388.8: five in European countries, you know, five in, you know,
North
5388.8 --> 5391.7: America, something like that. So we can have this truly
5391.7 --> 5396.4: distributed global test a bit by utilizing, by leveraging
 the
5396.4 --> 5401.7: Japanese government budget or and the other budget. But I
 look
5401.7 --> 5407.5: here that how many nodes are appropriate? It's just a
5407.5 --> 5413.7: sampling, because Bitcoin has over 15,000 nodes. And of
5413.7 --> 5417.1: course, Ethereum has tons of nodes. But how many, you kno
w,
5417.8 --> 5422.0: full nodes or how many nodes we should have for the other
 test
5422.0 --> 5430.1: a bit? So that is my technology question. Of course, due
to the
5430.1 --> 5435.8: budget limitations, you know, the nodes operated by Japan
ese
5435.8 --> 5438.9: government, Japanese government budget is very limited. B
ut so
5438.9 --> 5442.0: if we need, you know, for example, 100 nodes in the world,
5442.6 --> 5446.6: so we need to ask some other parties to collaborate with
to
5446.6 --> 5451.8: operate that node for six months. Do you have any idea ho
w

5451.8 --> 5453.3: many nodes are appropriate?
5454.7 --> 5458.2: What's the, so what is the benefit of more nodes?
5459.8 --> 5464.8: Yeah, if it is just three nodes, I think it's not good, y
ou know,
5465.3 --> 5467.2: for the, you know, distributed network.
5467.8 --> 5473.4: Okay, I understand. So it's about being able to prove tha
t
5474.1 --> 5478.8: the evaluation is appropriate for the level of decentrali
zation.
5479.0 --> 5480.5: Yes. Okay.
5482.3 --> 5487.8: Well, I assume it would be, we should decide a ratio. If
that's
5487.8 --> 5488.2: the case.
5488.4 --> 5489.8: It's a kind of sampling, but
5489.8 --> 5490.8: Yeah, okay.
5490.8 --> 5492.9: Yeah, I don't know.
5492.9 --> 5496.0: We have the three nodes in Asia, three nodes in North Ame
rica or
5496.0 --> 5497.2: something like that.
5502.3 --> 5505.1: But so, you know, Japanese government would like to know
5505.1 --> 5509.3: that, so how many nodes we need and how many nodes Japane
se
5509.3 --> 5510.9: government should support.
5511.4 --> 5518.4: And are the nodes to be only controlled by BIG-IN or can
other
5518.4 --> 5521.7: organizations offer to provide?
5521.9 --> 5525.5: For example, if we need, you know, 1,000 nodes for this
5525.5 --> 5528.0: evaluation, but, you know, Japanese government doesn't ha
ve
5528.0 --> 5531.7: that, you know, budget for that. So we need to, you know,
 have
5531.7 --> 5533.0: some collaboration with other party.
5534.3 --> 5540.0: Okay. So we should work out what the minimum node number
for
5540.0 --> 5540.4: BIG-IN?
5540.6 --> 5546.3: But so that is another thing I need to, you know, work wi
th the
5546.3 --> 5551.2: owner that, so if the Ethereum Foundation has some idea t
o help
5551.8 --> 5556.0: operating other nodes, it might be a potential collaborat
ion.
5556.8 --> 5560.7: Yes, we need to figure out how many nodes actually they a
re
5560.7 --> 5565.4: running right now. And then maybe they have, for example,
 if
5565.4 --> 5568.5: they have 10 nodes for each continent, you know, we can
5568.5 --> 5573.1: borrow each one and maybe it doesn't, you know, break the
5573.1 --> 5578.8: consensus. So I, yeah, I think that kind of direction is
good
5578.8 --> 5579.3: idea.

5583.5 --> 5587.0: Okay, so we are running out of time for today's discussio
n, but
5587.0 --> 5590.7: we are happy to any input about that, this kind of thing,
5590.8 --> 5593.3: because that is so we need to decide that in a budget pla
n for
5593.3 --> 5599.2: that. But so we are so we are welcome any input by email
or by
5599.2 --> 5603.0: any input over there, this question or something like tha
t.
5603.1 --> 5607.4: But we need that kind of input. That kind of input is not
5607.4 --> 5607.8: possible.
5614.4 --> 5617.5: Thank you everyone for it's been like a really great disc
ussion.
5618.0 --> 5621.7: Off the top of my head, the next steps is the call for pa
pers is
5621.7 --> 5628.2: going to be socialized officially in August, but we'll sh
are some
5629.0 --> 5633.2: socialization of it beforehand to be ready. And then the
key
5634.3 --> 5642.9: event will be in October. The symposium where we yeah, fo
rward
5642.9 --> 5646.1: the progress towards the start of the competition next ye
ar.
5647.6 --> 5648.1: Thank you.
5650.2 --> 5654.4: And we have 10 minutes break. And so we have that another
5654.4 --> 5658.2: discussion on the key management, but it's it's a
5659.1 --> 5662.5: review discuss about key management for us, you know, the
5662.5 --> 5666.2: key management part of this competition, that how he what
5666.2 --> 5670.0: kind of key management mechanism so we should target for
the
5670.0 --> 5672.3: competition or what is the scope of competition with key
5672.3 --> 5672.8: management part.
5674.7 --> 5678.5: Anyway, we have that 10 minutes break and let's resume th
is the
5678.5 --> 5680.4: next session at 1110.
5696.3 --> 5699.1: Thank you very much for remote participant, including And
y.
5699.2 --> 5699.5: Thank you.