RENCONTRE TECHNIQUE A BORDEAUX DU 11 au 13 NOVEMBRE 2022

CONFERENCE D'ELOIS SUR BABE/GRANDPA

BABE: BABE — Research at W3F 1
GRANDPA: https://research.web3.foundation/en/latest/polkadot/finality.html

Montage vidéo et timeline → Bertrand

00:00 définition du consensus BABE/GRANDPA
01:51 question de 1000i100 : qui vote pour le set des autorités ?
03:00 définition d'une session
03:40 comment choisir la durée de la session ?
05:47 question de Manutopik : token ?
06:11 stabilité du réseau ? → cf GRANDPA
07:06 BABE - GRANDPA, un consensus hybride
09:27 VRF (verifiable random function)
09:41 session keys (dont une pour BABE)
10:25 slots (6 secondes)
10:49 éligibilité pour les blocs primaires
12:22 blocs secondaires, un « modulo à la con »
12:46 règles de priorité
14:40 règle de résolution des forks
15:35 questions sur BABE
15:40 consensus sur le temps ?
17:06 remarque sur GRANDPA (non)
17:27 création du DU en nombre de bloc ?
17:59 validation des transactions ?
20:30 la transaction doit-elle avoir une info de la blockchain ?
22:01 quid de l'accusé de réception dans un wallet ?
24:09 remarque de Poka sur timeout
24:59 est-ce que la VRF a un rôle dans GRANPA ?
25:11 qu'est-ce qu'une VRF ?
25:54 question les blocs vide sont-ils liés à un trafic réseau ?
26:41 question sur l'ajustement du seuil de la VRF
27:15 est-ce que seuil dépend du nombre d'autorités ?
27:56 le résultat de la VRF n'est pas anticipable ?
28:38 comment attaquer le réseau ?
28:51 On va passer à GRANDPA
30:16 on ne peut pas voter pour 2 branches différentes
31:09 si on « DDOS » 40% des autorités ?
31:36 quels sont les critères de vote ?
31:58 Quel nœud va voter ?
32:16 les transactions sont dans les 3 branches ?
32:36 si il y a un souci du réseau internet
33:09 tout ça se fait toutes les 6 secondes ?
34:17 à partir de combien de temps on peut se rendre compte qu'une transaction n'a pas été notée dans un block ?
34:54 est-ce que l'utilisateur est notifié de la validation de transaction ?
35:45 que se passe-t-il si grosse coupure électrique nationale ?
36:42 au niveau des sessions ?
37:50 GRANDPA ne gère pas le temps Blockchain
40:21 le temps pose question, soit avancement du temps Blockchain soit le nombre de blocks

41:41 sur le DU, demande de précision du temps comptabilisé. Block toutes les 6 secondes ?
44:21 Pourquoi ces 2 noms BABE/ GRANDPA ?
44:57 Pourquoi on n'utilise pas mieux les sessions ?
45:49 des papiers existent sur BABE et GRANDPA qui donnent des détails
46:15 une attaque par le contrôle des horloges des ordinateurs ?
48:00 le calcul d'une VRF demande beaucoup d'énergie, comme une POW ?
48:27 c'est donc efficient en consommation d'énergie ?
48:40 et au niveau de la bande passante ?
49:44 ça fait beaucoup de notifications toutes les 6 secondes ?
50:26 tous les échanges entre nœuds de la blockchain sont filaires
50:46 différence entre « full node » et « light node »
51:47 changement des sets des autorités, lié au consensus
53:23 le set des autorités change toutes les heures ?
53:51 qu'est-ce qui se passerait si on installait un « full node » sur un mobile ?
55:14 sortir de la confusion « full node », « autorité » et « light node »
55:51 nuance entre « autorité » et « validateur »
56:53 redondance d'identité dans un nœud
57:30 il y a 3 types d'offenses (dans BABE, dans GRANDPA, dans une session)
58:20 on peut faire un noeud « validateur actif » + un nœud « back-up »
59:07 on sauvegarde les « sessions keys » dans 1 des 2 dossiers
59:25 offense « I'm online »
1:00:55 quid des « nœuds archives » ?
1:01:27 y a-t-il un moyen de configurer un « light node » pour travailler l'un des deux BABE et/ou GRANDPA ?
1:02/21 tu peux mettre en pause un « light node »
1:02:28 « light node » et « small dot » c'est pareil ?
1:03:12 certaines offenses sont plus ou moins sévères ? Mettre en place un comité technique humain pour sortir de la « black list » ?
1:04:13 précisions sur les offenses « I'm online »
1:06:43 les offenses graves sur BABE et GRANDPA : blacklisté et un comité technique fait sortir ou pas de la liste
1:07:21 le monde des forgerons est incité financièrement à forger un block
1:10:11 il y a 2 rémunérations : 1 fixe (avec ou sans activité de transactions) + 1 variable (en fonction de l'activité)
1:11:04 tu peux filtrer le trafic entrant ?
1:11:34 compiler des blocks vides pour gagner plus d'argent ?
1:13:01 toute blockchain doit avec une rémunération variable basée sur l'activité du réseau
1:13:17 précisions sur la VFR par rapport au block vide
1:14:55 est-il possible de faire de la rétention de transaction et éviter certains blocks ?
1:16:21 la résolution actuelle est l'application des 2 rémunérations
1:17:17 la Trésorerie peut venir en complément d'un membre qui n'aurait pas assez de liquidité pour une transaction. Quid d'une Trésorerie à sec pour les validateurs ?
1:18:23 à quel moment cela casserait la TRM par rapport à une promesse future de fonds disponibles dans la Trésorerie ?
1:19:10 comment sont calculés les frais de transaction ?
1:21:04 que se passe-t-il si les flux de transaction financière sont supérieurs aux capacités du réseau ?
1:21:16 si on a un spam de micro-transactions pour faire tomber le système ?
1:22:07 dans BABE, quid des 2 secondes + 2 secondes + 2 secondes ?
1:23:51 ce sont des frais de transaction ou des frais d'événement ?
1:25:47 on peut parler de « frais d'exécution »
1:26:05 est-ce que cela serait intéressant d'ajouter une taxe aux gros mouvements de fonds ?
1:27:53 Ce n'est pas aux développeurs de décider d'appliquer une taxe ou pas…

1:28:42 Plutôt qu'une taxe sur les montants, opter un pour nombre d'exécutions gratuit par membre ?
1:30:08 comment une taxe, techniquement, peut détecter les transactions en petites coupures d'un grand transfert de fond ?
1:30:11 mettons 5% de taxe…
1:30:48 il y a d'autres problématiques avec les frais variables
1:32:15 ça va servir à financer les nœuds forgerons !
1:33:00 l'idée de quotas n'est pas urgente pour la migration technique V1 vers V2, comme pour les taxes des gros transferts de fonds
1:33:39 mais c'est important en terme de communication (pour les financements participatifs…)
1:33:58 vu le peu de ressource humaine pour le dev de la V2, il faut assumer le fait qu'il n'y aura pas de quota au moment de la migration mais qu'il sera possible d'en installer plus tard
1:34: 32 est-ce que les frais d'exécution sont élevés ?
1:35:29 il faut trouver une formule simple : tant de poids de calcul = tant de frais
1:36:11 et si nous fixions une constante ?
1:37:44 quid des prélèvements automatiques ?
1:37:50 l'app pourrait avertir l'utilisateur de l'état du réseau (frais élevés ou normaux) ?
1:38:38 dans la pratique, le réseau blockchain revient vite « à la normale »
1:39:26 on sort du consensus, au sujet des transactions de prélèvement automatique, on est après la période de migration
1:40:21 on peut simuler le comportement de la V2
1:41:05 si après la v2 on a 5 à 10 ans pour développer les quotas…
1:42:03 Substrate ne fonctionne pas si les frais sont à 0
1:42:26 ce n'est pas l'open bar, les frais couvrent les dépenses CPU et autres
1:43:14 si après calcul, les frais ne sont pas à 1 centime mais à 1 DU ?
1:43:43 Délais, quotas : en fonction des ressources humaines disponibles !
1:44:28 pour simplifier la communication : sans frais initiaux ?
1:45:10 proposition de fixer une constante entre poids et frais
1:46: 01 cette constante ne peut pas être fixée en DU mais remise à jour
1:46:08 on raisonne en G1 mais nous devons raisonner en DU ?
1:46:28 nous pouvons ensuite raisonner sur la mise en place de quotas futurs
1:47:04 « le quota de frais non payé me parle bien »
1:47:23 proposer un jour aux membres une part de serveur à faire tourner en G1 ?
1:48:33 « un forgeron, c'est un administrateur système POINT »
1:49:07 ce qui est important au niveau communication, c'est qu'un forgeron a un pouvoir limité
1:49:44 un forgeron a une responsabilité technique
1:50:14 la gestion des frais et des quotas est un sujet politique
1:50:47 pour l'instant le comité technique a un pouvoir de veto
1:51:11 le comité d'éthique sera inscrit mais opérationnel après migration
1:51:34 organiser une rencontre utilisateurs pour décider les choix avant la date de migration
1:51:51 on peut commencer à appliquer une gouvernance off-chain pour les développeurs car ils sont peu nombreux et réputés entre-eux, pour tests
1:52:17 alors il faut communiquer correctement ! Pour sortir de la centralisation vers la décentralisation
1:53:06 si on est bloqué on peut « forker »
1:53:18 Substitute permet de changer la donne si +70% des forgerons sont OK
1:54:14 ça parait donc important d'inscrire dans la licence des futurs forgerons
1:54:58 c'est pour ça qu'en cas de problème, le forgeron s'engage à donner ses coordonnées pour la communauté
1:55:31 la communauté doit être capable de contacter au moins 66% des forgerons
1: 56:09 faudrait refaire une migration si la Blockchain est bloquée ?!
1:57:12 ça peut se passer aussi avec la migration V1 vers V2 !