GPBFT Πρωτόκολλο - Επισκόπηση, Διαφορές με PBFT, και Επεξήγηση Κώδικα

Εισαγωγή στο GPBFT

Το Πρωτόκολλο Ομαδικής Πρακτικής Βυζαντινής Ανοχής Σφαλμάτων (GPBFT) είναι μια επέκταση του πρωτοκόλλου PBFT. Το GPBFT στοχεύει στη βελτίωση της αποδοτικότητας και της κλιμάκωσης στους μηχανισμούς συναίνεσης blockchain μέσω της εισαγωγής ομαδικών υπογραφών και βελτιωμένης παρακολούθησης κακόβουλων κόμβων.

Αναφορά: https://onlinelibrary.wiley.com/doi/10.1155/2022/8311821

Βασικές Διαφορές μεταξύ GPBFT και PBFT

1. Καθυστέρηση Συναίνεσης: Το GPBFT εισάγει μια φάση GroupSign για τη μείωση της συνολικής καθυστέρησης συναίνεσης.
2. Επικοινωνιακή Επιβάρυνση: Χρησιμοποιεί σύντομες ομαδικές υπογραφές για να ελαχιστοποιήσει την επικοινωνιακή επιβάρυνση.
3. Ασφάλεια και Ανοχή Σφαλμάτων: Οι διπλές διαχειριστικές σύντομες ομαδικές υπογραφές ενισχύουν την ασφάλεια και την ανοχή σφαλμάτων.
4. Αποδοτικότητα Παρακολούθησης: Περιλαμβάνει έναν Διαχειριστή Ομαδικής Παρακολούθησης για την αποτελεσματική ανίχνευση και αποκλεισμό κακόβουλων κόμβων.
5. Κλιμάκωση: Το GPBFT έχει σχεδιαστεί για να είναι πιο κλιμακωτό, χειριζόμενο μεγαλύτερα δίκτυα πιο αποτελεσματικά.

Τροποποιήσεις στο PBFT για τη Δημιουργία του GPBFT

1. Προστέθηκαν οι φάσεις GroupSign και Trace στο πρωτόκολλο.
2. Εφαρμόστηκε η συνάρτηση group_sign για τη διαχείριση των ομαδικών υπογραφών.
3. Προστέθηκε η συνάρτηση trace για την ανίχνευση και διαχείριση κακόβουλων κόμβων.
4. Ενημερώθηκε η συνάρτηση handle_event για να συμπεριλάβει νέα μηνύματα: group_sign και trace.
5. Ενισχύθηκε η συνάρτηση state_to_string για να αντικατοπτρίζει νέες καταστάσεις και μηνύματα.
6. Τροποποιήθηκε η συνάρτηση reset_msgs για την επαναφορά των μηνυμάτων ομαδικών υπογραφών.

Επεξήγηση Κώδικα GPBFT

1. set_state(node): Αρχικοποιεί την κατάσταση του κόμβου για το GPBFT, συμπεριλαμβανομένων των ομαδικών υπογραφών και των πληροφοριών ανίχνευσης.
2. state_to_string(node): Επιστρέφει μια αναγνώσιμη συμβολοσειρά που περιγράφει την τρέχουσα κατάσταση του κόμβου, συμπεριλαμβανομένων των νέων καταστάσεων και μηνυμάτων.
3. reset_msgs(node): Επαναφέρει τα μηνύματα στην κατάσταση του κόμβου, συμπεριλαμβανομένων των ομαδικών υπογραφών.
4. get_miner(node, round_robin=True): Υπολογίζει τον νέο κόμβο εξόρυξης βάσει κυκλικής σειράς ή κατακερματισμού του τελευταίου μπλοκ.

5. init(node, time=0, starting_round=0): Αρχικοποιεί την κατάσταση του κόμβου και ξεκινά έναν νέο γύρο.
6. create_GPBFT_block(node, time): Δημιουργεί ένα νέο μπλοκ για το πρωτόκολλο GPBFT, συμπεριλαμβανομένων των απαραίτητων συναλλαγών και δεδομένων.
7. handle_event(event): Διαχειρίζεται συμβάντα που σχετίζονται με το πρωτόκολλο GPBFT, συμπεριλαμβανομένων νέων μηνυμάτων group_sign και trace.
8. validate_message(event, node): Επαληθεύει αν ένα μήνυμα είναι έγκυρο για τον κόμβο.
9. process_vote(node, type, sender): Καταγράφει ψήφους για προετοιμασία και επιβεβαίωση μηνυμάτων.
10. pre_prepare(event): Ξεκινά τη φάση προετοιμασίας για το προτεινόμενο μπλοκ.
11. prepare(event): Διαχειρίζεται τη φάση προετοιμασίας.
12. commit(event): Διαχειρίζεται τη φάση επιβεβαίωσης.
13. group_sign(event): Διαχειρίζεται τα μηνύματα ομαδικών υπογραφών.
14. trace(event): Διαχειρίζεται την ανίχνευση κακόβουλων κόμβων.
15. new_block(event): Διαχειρίζεται τη δημιουργία νέων μπλοκ.
16. init_round_change(node, time): Αρχικοποιεί μια αλλαγή γύρου.
17. start(node, new_round, time): Ξεκινά έναν νέο γύρο.
18. timeout(event): Διαχειρίζεται καταστάσεις χρονικών ορίων για τον κόμβο.
19. schedule_timeout(node, time, remove=True, add_time=True): Προγραμματίζει ένα χρονικό όριο για τον κόμβο.
20. resync(node, payload, time): Διαχειρίζεται δράσεις επανασυγχρονισμού συγκεκριμένες για το GPBFT.
21. clean_up(node): Καθαρίζει συμβάντα που σχετίζονται με το πρωτόκολλο GPBFT από την ουρά συμβάντων του κόμβου.

Αναλυτική Εξήγηση του Αλγορίθμου GPBFT:

Το GPBFT (Group Practical Byzantine Fault Tolerance) είναι μια επέκταση του PBFT (Practical Byzantine Fault Tolerance) που έχει σχεδιαστεί για να βελτιώσει την αποδοτικότητα και την κλιμακωσιμότητα των μηχανισμών συναίνεσης στα blockchain. Παρακάτω εξηγείται αναλυτικά ο αλγόριθμος GPBFT και οι διαφορές του με το PBFT.

Αρχική Κατάσταση και Ρυθμίσεις:

Αρχικοποίηση Κατάστασης (set_state):

Κατά την εκκίνηση του αλγορίθμου, η κατάσταση του κόμβου αρχικοποιείται. Περιλαμβάνει πληροφορίες για τον τρέχοντα γύρο, το προτεινόμενο block, τα μηνύματα που έχουν ληφθεί, και τις πληροφορίες ανίχνευσης κακόβουλων κόμβων.

Φάσεις του Αλγορίθμου GPBFT:

Φάση Pre-Prepare:

Όταν ένας κόμβος γίνεται προτείνων (proposer), δημιουργεί και προτείνει ένα νέο block. Το block αυτό διανέμεται στους άλλους κόμβους μέσω μηνύματος `pre_prepare`.

Οι κόμβοι που λαμβάνουν το μήνυμα επαληθεύουν το block και, εάν είναι έγκυρο, αλλάζουν την κατάστασή τους σε `pre-prepared` και στέλνουν μηνύματα `prepare`.

Φάση Prepare:

Οι κόμβοι συγκεντρώνουν τα μηνύματα `prepare` από άλλους κόμβους. Όταν ένας κόμβος λάβει αρκετά μηνύματα `prepare` (από τουλάχιστον 2f + 1 κόμβους, όπου f είναι ο αριθμός των κακόβουλων κόμβων που μπορεί να ανεχθεί το σύστημα), αλλάζει την κατάστασή του σε `prepared`.

Στη συνέχεια, στέλνει μηνύματα `commit` στους άλλους κόμβους.

Φάση Commit:

Οι κόμβοι συγκεντρώνουν τα μηνύματα `commit`. Όταν ένας κόμβος λάβει αρκετά μηνύματα `commit`, αλλάζει την κατάστασή του σε `committed` και το block προστίθεται στην αλυσίδα.

Στη συνέχεια, οι κόμβοι μπορούν να ξεκινήσουν έναν νέο γύρο.

Φάση GroupSign:

Αυτή η φάση είναι μοναδική στο GPBFT και περιλαμβάνει τη συλλογή ομαδικών υπογραφών από τους κόμβους. Οι κόμβοι στέλνουν μηνύματα `group_sign` για να επιβεβαιώσουν ότι συμφωνούν με το block.

Όταν συγκεντρωθούν αρκετές ομαδικές υπογραφές, η κατάσταση αλλάζει σε `group_signed`.

Φάση Trace:

Αυτή η φάση περιλαμβάνει την ανίχνευση κακόβουλων κόμβων. Οι κόμβοι στέλνουν πληροφορίες ανίχνευσης μέσω μηνυμάτων `trace`.

Εάν εντοπιστούν κακόβουλοι κόμβοι, αυτοί αποκλείονται από το δίκτυο.

Διαχείριση Χρόνου και Timeout:

schedule_timeout: Η συνάρτηση αυτή προγραμματίζει ένα γεγονός timeout για να διασφαλίσει ότι οι κόμβοι δεν θα περιμένουν απεριόριστα για

μηνύματα. Εάν δεν ληφθούν αρκετά μηνύματα εντός του καθορισμένου χρόνου, ο κόμβος προχωράει στον επόμενο γύρο.

Λειτουργία του Αλγορίθμου PBFT:

Το PBFT (Practical Byzantine Fault Tolerance) είναι ένας αλγόριθμος συναίνεσης που επιτρέπει σε ένα κατανεμημένο σύστημα να φτάσει σε συμφωνία ακόμα και αν μερικοί κόμβοι είναι κακόβουλοι ή παρουσιάζουν σφάλματα. Παρακάτω περιγράφεται η λειτουργία του PBFT βήμα προς βήμα.

Βασικές Αρχές:

Ανοχή σε Σφάλματα: Ο αλγόριθμος PBFT μπορεί να αντέξει έως και fff κακόβουλους κόμβους σε ένα σύστημα με 3f+13f + 13f+1 συνολικούς κόμβους.

Στάδια Συναίνεσης: Ο αλγόριθμος χωρίζεται σε τρία κύρια στάδια: Pre-Prepare, Prepare και Commit.

Βήματα του Αλγορίθμου PBFT:

Προετοιμασία (Pre-Prepare Stage):

Ο κόμβος που είναι υπεύθυνος για την πρόταση (primary node ή leader) δημιουργεί μια πρόταση (ένα block) και στέλνει ένα μήνυμα `pre_prepare` σε όλους τους άλλους κόμβους (replicas).

Το μήνυμα περιέχει τα στοιχεία της πρότασης και ένα μοναδικό αναγνωριστικό.

Προετοιμασία (Prepare Stage):

Οι κόμβοι που λαμβάνουν το μήνυμα `pre_prepare` επαληθεύουν την πρόταση.

Αν η πρόταση είναι έγκυρη, οι κόμβοι στέλνουν μηνύματα `prepare` σε όλους τους άλλους κόμβους.

Κάθε κόμβος συγκεντρώνει τις ψήφους `prepare` από τους άλλους κόμβους.

Όταν ένας κόμβος λάβει 2f+12f + 12f+1 μηνύματα `prepare` (συμπεριλαμβανομένου του δικού του), αλλάζει την κατάστασή του σε `prepared`.

Δέσμευση (Commit Stage):

Όταν ένας κόμβος είναι `prepared`, στέλνει μηνύματα `commit` σε όλους τους άλλους κόμβους.

Οι κόμβοι συγκεντρώνουν τις ψήφους `commit` από τους άλλους κόμβους.

Όταν ένας κόμβος λάβει 2f+12f + 12f+1 μηνύματα `commit` (συμπεριλαμβανομένου του δικού του), αλλάζει την κατάστασή του σε `committed`.

Το block προστίθεται στην αλυσίδα (blockchain) και οι κόμβοι είναι έτοιμοι να επεξεργαστούν το επόμενο block.

Αντιμετώπιση Σφαλμάτων:

Αν ο πρωτεύων κόμβος (primary) αποτύχει ή είναι κακόβουλος, οι άλλοι κόμβοι μπορούν να ανιχνεύσουν την αποτυχία και να ξεκινήσουν μια διαδικασία αλλαγής γύρου (view change).

Στη διαδικασία αλλαγής γύρου, ένας νέος κόμβος αναλαμβάνει ως πρωτεύων και η διαδικασία συναίνεσης επαναλαμβάνεται.