Diavgeia & Bitcoin

Αυτό που θέλουμε να προσθέσουμε στην Διαύγεια, είναι κάποιου είδους εγγύηση ότι σε βάθος χρόνου οι αποφάσεις θα μείνουν αμετάβλητες (immutability). Για να γίνει αυτό, θα χρησιμοποιήσουμε το Bitcoin και όχι κάποιο private blockchain, όπως λέγαμε αρχικά, καθώς το τελευταίο είναι censored και δεν μας εξασφαλίζει σε καμία περίπτωση τα ίδια επίπεδα immutability με αυτά ενός public blockchain. Ο τρόπος με τον οποίο θα μπαίνουν οι αποφάσεις της Διαύγειας στο Bitcoin, είναι ο εξής:

1. Οι φόρεις βάζουν στην Διαύγεια τις αποφάσεις τους και σε συγκεκριμένα, προκαθορισμένα χρονικά διάστηματα (π.χ. 1 φορά την μέρα), η Διαύγεια έχει την υποχρέωση να βάλει αυτές τις αποφάσεις στο Bitcoin.
2. Όταν έρθει η στιγμή για την Διαύγεια να βάλει τις αποφάσεις στο Bitcoin, θα συμπεριλάβει μόνο τις καθημερινές αποφάσεις στο blockchain. Θα φτιάξει από αυτές το Merkle Tree, θα υπογράψει και θα βάλει το root αυτού στο Bitcoin. Το transaction που θα γίνει στο Bitcoin θα έχει ρόλο proof of burn (καθώς δεν θα μεταφέρονται χρήματα όπως γίνεται στην πλειοψηφία των συναλλαγών), δηλαδή είναι μια απόδειξη ότι υπήρξε το root της Διαύγειας στο Bitcoin.
3. Η Διαύγεια αφού βάλει τα δεδομένα στο Bitcoin θα πρέπει να δημοσιεύσει στο site της το Merkle Tree (ώστε να ξέρουμε με ποια σείρα πήρε τις αποφάσεις, από τις οποίες προέκυψε η ρίζα που μπήκε στο Bitcoin) καθώς και το transaction του Bitcoin (ώστε να μπορούν να το δουν οι φορείς / πολίτες μέσα από το blockchain του Bitcoin).

Επίσης, να πούμε τα εξής:

- Στην production έκδοση της Διαύγειας, μπορούν να σβηστούν αποφάσεις. Αυτές είναι οι αποφάσεις που είτε περιέχουν ευαίσθητα δεδομένα (π.χ. κάποιος υπάλληλος που πέρασε από πειθαρχικό) και μαρκάρονται ως τέτοιες κατά την φάση του upload, είτε όταν κάποιος "επικαλεστεί" ότι ανέβασε ένα εντελώς "λανθασμένο έγγραφο" στην Διαύγεια (https://diavgeia.gov.gr/faq/post -> Ορθή επανάληψη - Ανάκληση - Διόρθωση δεδομένων -> Ανάκληση ανάρτησης). Στην τωρινή έκδοση αυτό το μαρκάρισμα των ευαίσθητων δεδομένων φαίνεται μόνο στα μεταδεδομένα (όχι στο text του pdf), αλλά πλέον στο rdf τα μεταδεδομένα με το text έχουν πρακτικά συγχωνευτεί στο ίδιο αρχείο. Όμως επειδή η διαγραφή θα δημιουργούσε πρόβλημα inconsistency με το Bitcoin, στο Merkle Tree ΔΕΝ συμπεριλαμβάνονται όσες πράξεις περιέχουν ευαίσθητα δεδομένα. Τώρα σχετικά με το "λανθασμένο έγγραφο", πραγματικά μου φαίνεται σαν "παραθυράκι", ώστε να διαγράφονται πράξεις από την Διαύγεια. Προσωπικά σέβομαι το privacy και για αυτό πιστεύω ότι δεν πρέπει να μπαίνουν στο bitcoin αυτές οι πράξεις που έχουν ευαίσθητα δεδομένα, αλλά οι αποφάσεις που είναι λανθασμένες, ας παραμένουν για πάντα στην Διαύγεια σαν λανθασμένες και ας μπαίνουν στο bitcoin. Αν ο λόγος που σβήνονταν οι αποφάσεις ήταν για space needs, νομίζω ότι δεν υπάρχει αυτή η δικαιολογία πλέον με το rdf.

- Η Διαύγεια θα έχει μόνο μια και μοναδική public address στην οποία θα φαίνονται τα transactions που κάνει. Αυτή η διεύθυνση θα δημοσιευθεί μια φορά και θα υπάρχει για πάντα στην Διαύγεια αμετάβλητη. Αυτό θα μας γλυτώσει από την περίπτωση που η Διαύγεια έκανε 2 commits στο Bitcoin με διαφορετικά merkle trees (ξέροντας εξαρχής ποια πράξη θα αλλάξει / διαγράψει), αντικαθιστώντας σε βάθος χρόνου το "καλό" merkle tree της πρώτης διεύθυνσης με το "κακό" merkle tree της δεύτερης διεύθυνσης. Έχοντας μια διεύθυνση, οι πολίτες / φορείς θα ξέρουν ότι μόνο 1 commit την ημέρα και από την συγκεκριμένη διεύθυνση είναι valid.

- Αυτό που πρέπει να γίνει κατανοητό είναι ότι η χρήση του Bitcoin δεν προσφέρει τίποτα άλλο παρά immutability,για την περίπτωση διαγραφής ή αλλοίωσης των αποφάσεων. Κάτι τέτοιο το εγγυάται προφανώς και η ψηφιακή υπογραφή, στην περίπτωση που κάποιος έχει κατεβάσει το pdf και το κρατήσει για πάντα στο pc του. Όμως, σε περίπτωση που διαγραφεί αυτό το pdf από τον φορέα, δεν υπάρχει η εγγύηση ότι δεν θα αλλοιωθεί στην συνέχεια. Εμείς θέλουμε να μειώσουμε αυτό το timespan που μπορεί να αλλοιωθεί μια πράξη. Ιδανικά οι φορείς θα μπορούσαν να έχουν κατεβασμένη την απόφαση μαζί με την ψηφιακή υπογραφή και με το που περάσει στο Bitcoin, να την διαγράψουν από το pc τους, καθώς πλέον θα γνωρίζουν ότι δεν μπορεί να αλλοιωθεί η απόφασή τους.

- Ιδανικά θα μπορούσε να υπάρξει και ένας Validator, όπου θα έβλεπε όλα τα daily commits της Διαύγειας στο Bitcoin, και θα συνέκρινε για κάθε μέρα το merkle root του Bitcoin με το merkle tree που θα κατασκεύαζε από τις αποφάσεις. Έτσι κάποιος θα μπορούσε να δει αν όντως είναι consistent η Διαύγεια από την αρχή λειτουργίας της μέχρι και σήμερα. Αυτή να είναι ίσως μια καλή ιδέα για τον 3ο μήνα του έργου :)