

dentelle possible. Ils finissent par concevoir des machines spécialisées pour faire efficacement les rubans demandés et réussissent à diminuer les coûts de fabrication. À la longue, certains d'entre eux disposent de multiples machines performantes et fabriquent des longueurs énormes de

Comparée à la preuve d'enjeu, la preuve de travail semble catastrophique

rubans pourtant destinés à être détruits. Ils deviennent ce que nous appellerons des «industriels des rubans». Ils sont concurrents et les joueurs qui fabriquent les rubans à la main voient leur part de l'attribution diminuer de semaine en semaine et même devenir négligeable, car les industriels des rubans s'emparent de la presque totalité de S à chaque distribution.

La concurrence entre les industriels des rubans engendre un problème de rentabilité. Un industriel ne gagne une somme G , lors de la distribution hebdomadaire de la somme S , que s'il dépense pour la fabrication des rubans une somme qui se rapproche de G . En effet, si la fabrication pour gagner G coûte sensiblement moins que G , des concurrents attirés par le bon rendement de ce type d'investissement développent leurs outils et entrent sur le marché, ce qui fait baisser le rendement. À la longue, le rendement de la fabrication des rubans diminue et par exemple conduit les industriels du ruban à dépenser 80% (peut-être plus) de la somme G qu'ils gagnent chaque semaine en coût de production des rubans. Globalement, à cause de la compétition, les industriels des rubans qui se sont presque emparés de la totalité de la somme S distribuée chaque semaine dépensent par exemple 80% de S chaque semaine pour produire les rubans qui leur rapportent donc collectivement 20% de S . Le rendement sous cette hypothèse est de 25% (20% comparé à 80%), ce qui est suffisant pour que l'activité se poursuive. L'équilibre évoluera peut-être et la concurrence suscitera des progrès dans la fabrication des rubans, mais le rendement des investissements des industriels des rubans sera toujours assez réduit, par exemple 25% ou moins si la concurrence devient plus féroce.

La situation est en réalité devenue absurde: au lieu de distribuer chaque semaine la somme S , si on prend en compte les dépenses pour produire les rubans, chaque semaine c'est seulement 20% de S qui est réellement distribuée par le mécène. Non seulement il y a concentration de la distribution sur les industriels du ruban, mais en plus 80% de la somme S ou plus est en quelque sorte utilisée en pure perte pour fabriquer des rubans aussitôt détruits.

Comparée à la méthode de l'enjeu, la méthode du travail semble catastrophique et le mécène qui donne la somme S chaque semaine ne sera certainement pas satisfait qu'on distribue S par la méthode du travail. Les deux méthodes évitent la tricherie des enveloppes multiples, aucune des deux méthodes n'est parfaite, mais la méthode de l'enjeu est clairement meilleure.

VARIANTE À ENJEU CONFISQUÉ

On peut aussi imaginer que les sommes s_i ne sont pas rendues, mais confisquées. Un problème assez délicat en résulte. Chacun essaiera d'engager le plus d'argent possible en mettant une somme s_i élevée dans son enveloppe. Mais si le total de l'argent engagé par les joueurs est supérieur à S , alors la somme redistribuée sera inférieure à ce que les joueurs auront engagé et sacrifié; puisque l'argent redistribué à chacun est proportionnel à son enjeu, chaque joueur sera perdant. Le jeu deviendrait un peu fou car chacun serait tenté d'engager le plus possible en espérant que les autres engagent le moins possible. Une sorte de piège serait tendu aux joueurs qui risqueraient tous de perdre de

3

LES ATTAQUES SYBIL

Lorsqu'un système de communication accepte l'anonymat des utilisateurs, cela engendre des difficultés imprévues. Cela est apparu en informatique à l'occasion de la mise au point des réseaux pair-à-pair, c'est-à-dire sans administrateur central. La possibilité pour une même personne d'utiliser plusieurs pseudonymes différents lui procure des avantages assimilables à une tricherie, comme dans le cas de la distribution par la méthode S/N quand un joueur envoie plusieurs enveloppes. Sur les réseaux sociaux ou les forums, c'est par exemple un moyen de faire croire que plusieurs personnes soutiennent une même idée

alors qu'en réalité il n'y en a qu'une. Ce procédé est nommé «attaque Sybil». Ce nom provient du titre du livre *Sybil*, publié en 1973 par Flora Schreiber, qui raconte la vie de Shirley Mason, une femme qui aurait été atteinte d'un trouble dissociatif de l'identité, c'est-à-dire de personnalités multiples. Le nom d'«attaque Sybil» fut introduit en informatique par John Douceur en 2002. Le risque d'attaques Sybil a contraint Satoshi Nakamoto à introduire les preuves de travail dans la cryptomonnaie Bitcoin, bien que la solution des preuves d'enjeu introduite quelques années plus tard soit maintenant reconnue comme bien meilleure, ce que le jeu du mécène rend évident.