Ouvrir dans l'application

Virgile Griffith

811 abonnés Sur Suivre

La note que vous recherchez a été supprimée

Ethereum est une technologie qui change la donne, littéralement.

Virgile Griffith 29 mars 2019 · 6 min de lecture

Les gens demandent souvent : « A quoi sert Ethereum ? ". Les réponses précédentes à cette question incluaient souvent le terme « ordinateur mondial », mais malgré quelques exemples intéressants , il a été difficile de répondre à cette question à un niveau plus abstrait. Je propose une réponse à cette question. Je propose par la présente,

> Ethereum est une arène sans précédent pour jouer à des jeux coopératifs.

Et de plus,

> Ethereum permet des véhicules économiques puissants que nous ne comprenons pas encore.

La théorie des jeux non coopératifs , l'original et le plus wi d ely utilisé branche de la théorie des jeux, suppose l' *absence d'une autorité extérieure pour faire respecter les règles* . Fondamentalement, je prétends que le grand livre Ethereum constitue un **surveillant externe incorruptible, omniprésent qui,** quel que soit le jeu, est *toujours* disponible pour faire respecter les accords entre les joueurs. Cela implique qu'Ethereum, en théorie,

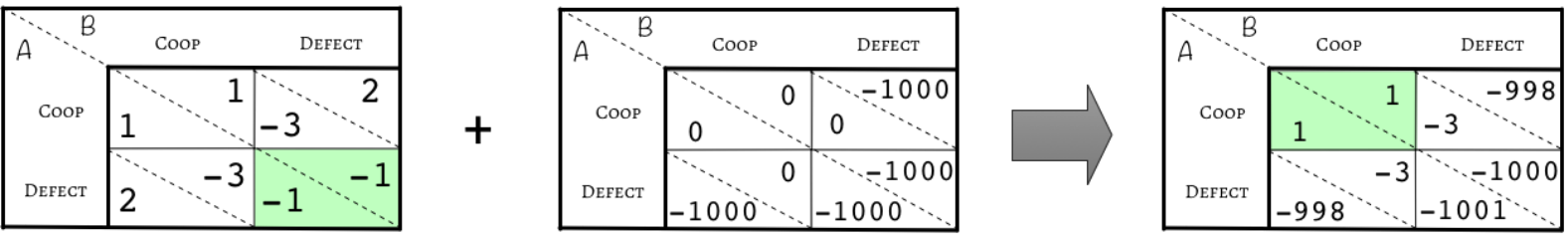
pourrait transformer *n'importe quel jeu* non coopératif en un jeu coopératif (parfois appelé jeu de coalition).

The transmogrification from non-cooperative to cooperative games is achieved by a technique we term *Game Warping* defined as using **transparent, triggerable, unstoppable burns and on-chain side-payments** to move game-theoretic equilibria or to create new player actions. Game Warping stacks as a new layer atop an uncooperative game to make cooperation the Rational choice.

Example 1: The Prisoner's Dilemma

The most well-known problem in game theory is the Prisoner's Dilemma—it is the quintessential example of a non-cooperative game in which the Rational strategy puts players into the worst possible state. Under Ethereum, I kid you not, the Prisoner's Dilemma *becomes a cooperative game*. Say players *A* and *B* want to do something naughty. But before they commit their crime, they each deposit one million dollars (valued at 1000 utility points) into a smart-contract which states, "If I publish a defect message, my million dollars gets destroyed." Now that the smart-contract is in place, as long as the police don't offer more than a million dollars to defect, Rational prisoners will choose to cooperate.

In the original Prisoner's Dilemma, Rational players will defect. But after the pay-off matrix has been *warped* to have a new equilibrium, Rational players will cooperate. See below,



Original Prisoners' Dilemma Game

Ethereum contract of burning any player who chooses to defect

Composite Game

Game Warping the Prisoner's Dilemma. Green denotes Nash equilibria.

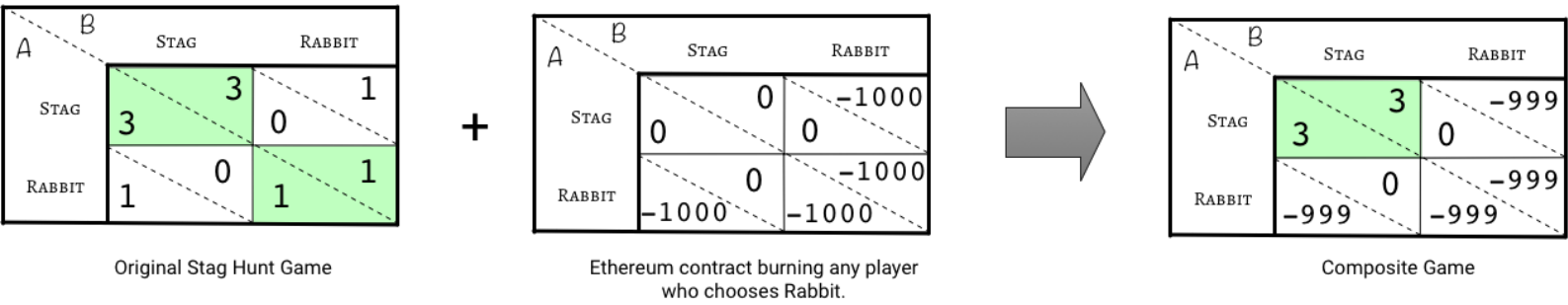
For inspiration, this list of situations matching the Prisoner's Dilemma includes: carbon-emissions, sports doping, tragedy of the commons, and international weapons buildup. Could Ethereum have something to offer these areas? It seems plausible.

Example 2: The Stag Hunt

The Stag Hunt is a canonical model of cooperation. The game posits two hunters choosing to hunt either *Stag* or *Rabbit*. The greatest pay-off is when both players hunt Stag (successfully hunting stag requires both hunters working together). But hunting

stag is also the riskier strategy because if the other hunter goes Rabbit, the hunter who went Stag gets nothing — the safer option is the guaranteed pay-off from hunting rabbit.

The desired warping is the same as the Prisoner's Dilemma. Each hunter deposits a large sum (worth 1000 utility points), that is burned if the hunter hunts Rabbit.



Original Stag Hunt Game

Ethereum contract burning any player who chooses Rabbit.

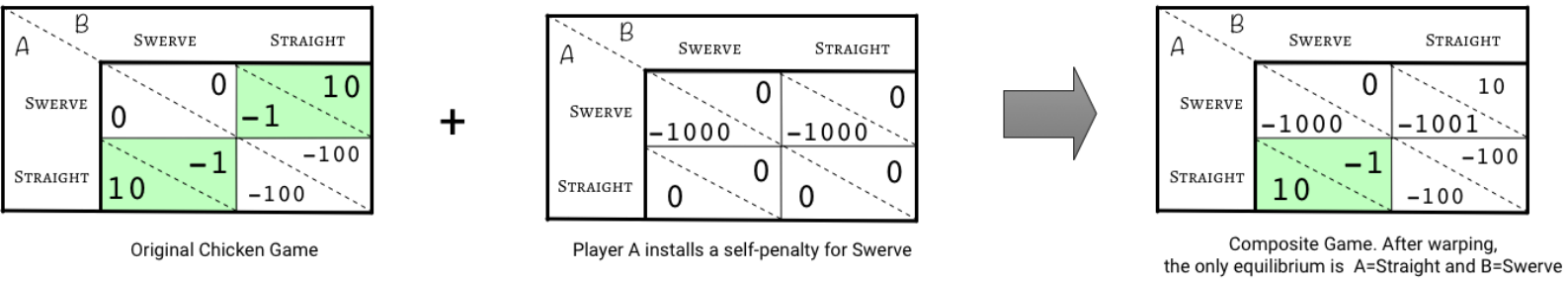
Composite Game

Game Warping the Stag Hunt. Green denotes Nash equilibria. Outcome is the same as in Prisoner's Dilemma and cooperation is now the sole equilibrium.

After warping, Rational hunters will now consistently choose Stag. There exist variations extensions of Stag Hunt to make the game more realistic, but the warp to turn it cooperative can always be done.

Example 3: The Chicken Game

In addition to warping games for collective benefit, a player can also warp games to gain a competitive advantage. We illustrate this with the game of Chicken. In this game, there are two players *A* and *B* and two actions, *Swerve* and *Straight*. Chicken exemplifies the sort of a game where *removing one of your options* (Swerve), the other player's Rational response is to your benefit. This removal can be done by making a large on-chain deposit which burns if you Swerve, this informs the other player that you, being a reasonable person, would never Swerve. This is the Ethereum equivalent of "publicly throwing away the steering wheel."



Original Chicken Game

Player A installs a self-penalty for Swerve

Composite Game. After warping, the only equilibrium is A=Straight and B=Swerve

Player A publicly warps his own actions to force player B into a choice between -1 utility for Swerve or -100 for Straight. Acting Rationally, Player B chooses to Swerve, and player A gains the reward.

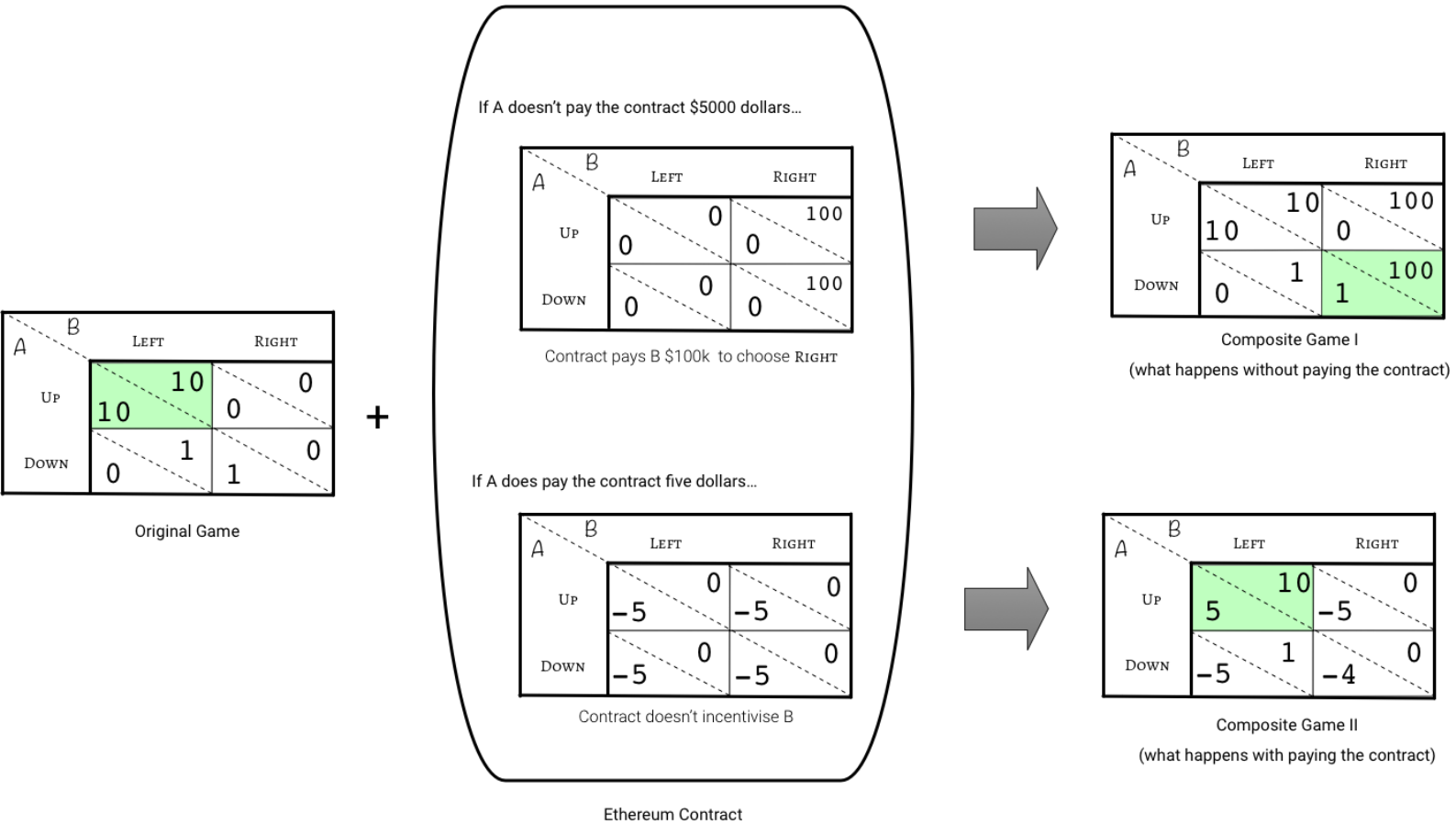
Chicken has two equilibria: [Straight,Swerve] and [Swerve,Straight]. But after the warp, the only remaining equilibrium is [Straight,Swerve], netting you (player A) the

maximum pay-off. In an Ethereum world, Chicken becomes a race for who can first publicly toss out one's own steering wheel.

Example 4: Warping Other Players' Games

Not limited to profiting from warping one's own games, one can even profit by threatening to warp games you're not even party to. Such extortion is obviously not endorsed, but we include it as a ramification of smart-contract technology. Consider the situation from this paper from Bono & Wolpert, where a third player *C* knows players *A* and *B* are about to play a game (and their pay-off matrix). With Ethereum, *C* can create a smart-contract in clear view of players *A* and *B*. This newly created contract states that unless *A* pays the contract, the contract will send a large payment to *B* conditional on *B* performing a rivalrous action against *A*. In essence, player *C* is extorting player *A* by credibly threatening to incentivize *B* to act rivalrous against *A*.

More concretely, consider the case below. Player *A* has actions *Up/Down* and player *B* has actions *Left/Right*. Initially, they both so desperately desire to occupy (Up, Left) in a very positive-sum interaction of ten utility points. However, an external player *C* recognizes the game about to be played and instantiates a smart-contract to extort $5000 (worth 5 utility points) from player *A*. If *A* does not pay the contract, the contract will pay *B* a hefty $100,000 (100 utility points) to choose *Right*. Once Player *A* sees the smart-contract, A is faced with the choice between two worse options — Composite Game I or Composite Game II. Unfortunately for player *A,* the Rational choice is Composite Game II, and A pays the extortion fee.



Contract extorting A to pay money so that the contract will refrain from incentivizing B to always go Right. Green denotes Nash equilibria. This game-warp is equivalent to the infamous p+epsilon attack.

One of the most surprising aspects of game-warping is that someone making a credible promise to pay can change the Rational strategy (and thus often the outcome of the game) without ever actually having to pay — if everyone plays Rationally, the game can be influenced *for free*!

Caveat. Ethereum payments and burns can only be triggered by an on-chain event. This is clearly a limitation — for example, in the prisoner's dilemma, if a prisoner could defect without it being broadcast on-chain, the player sidesteps the million-dollar burn. The relevance of side-channel (off-chain) communication will vary case-by-case. But the fewer off-chain interactions between players, the more likely the game can be successfully warped. The biggest contributions to this area will be discovering the exact property that games must have to ensure the player actions being warped will always be broadcast on-chain.

An additional caveat is that, for game-warping to succeed for individual gain, the recipient players must discover the warp has been performed; more precisely, the warp must become common knowledge. This limitation on anti-social contracts may turn out to be a blessing.

What does Ethereum change? Technically speaking, game-warping doesn't require smart-contracts. However, an obvious niche for Ethereum smart-contracts is for cases when, due to your jurisdiction or subject matter, reliably impartial judges are hard to find. Beyond these niches, Ethereum (or another smart-contract platform) makes *all* game-warping *vastly* more practical by providing a deterministic, all-seeing, cheap, and expedient (!) judge.

Ramifications. Ce framework fournit un processus pour générer des startups Ethereum. Par exemple on pourrait :

1. Parcourez un manuel classique de théorie des jeux .
2. Énumérez tous les jeux non coopératifs courants.
3. Voyez pour combien de ces jeux la coopération pourrait, via des paiements conditionnels ou des brûlures de dépôt, donner un équilibre supérieur aux équilibres de Nash d'origine.
4. Découvrez des industries importantes où ces jeux apparaissent.

5. Pour chaque industrie, déterminez si les actions des joueurs peuvent être transformées en événements en chaîne. Ensuite, pour chaque industrie résultante,
6. Soumettez une proposition de démarrage pour devenir un interlocuteur ConsenSys .

Sérieusement, vole cette idée.

Un merci spécial à Georgios , vi et Dan pour nos recherches conjointes sur le développement de la déformation du jeu et les commentaires sur les brouillons.

Merci à Daniel Moroz et Ying Tong .

Chaîne de blocs Ethereum La théorie des jeux

Sur Écrivez Aider Légal

Téléchargez l'application Medium

Download on the App Store GET IT ON Google Play