!DISCLAIMER!

Before you read this, I need to clarify a few things. First, this is simply a thought experiment. I wanted to answer the question of, “how could one use the blockchain to influence real world actions?” This paper covers a theoretical system with the potential to become real. This is by no means something that should be done. Secondly, I shouldn’t have to say this, but I don’t want to be held responsible for the next M.D. Chapman, so I’m saying it anyways: DO NOT MURDER PEOPLE! Murder is not only amoral, it is also ILLEGAL in every jurisdiction on the Planet. So despite what this paper talks about, do not murder anyone for any reason. MURDER IS BAD! So now that you know I don’t support murder and that this is just a thought experiment, here is my paper for your viewing pleasure.

Part I: Introduction

In his paper “Ethereum is game-changing technology, literally." , Dr. Virgil Griffith writes about how one can use smart contracts to introduce an impartial judge to make a non-cooperative game into a cooperative one. The issue with this impartial judge, and similarly constructed blockchain-based platforms, is that it is restricted to the blockchain - whereas most human behavior and judgement occurs on non blockchain based realities. Thus, the question to answer is: How do we incentivize as much interaction as possible on the blockchain to enforce the absoluteness and impartiality of the contract? My intent is that the system detailed in this paper could be that solution. It would be a system that would provide incentive to spend more tokens and value on the chain in order to manipulate the real world actions of any individual.

Looking at the greatest game of all, life and death, we can see how self-executing smart contracts can change vengeance (kill the guy who murdered me) into, ironically, a reduction of murder. Borrowing concepts from Jim Bell’s paper, “Assassination Politics”, which illustrated a manner to use smart contracts to murder people, Charon’s Obol provides an incentive to keep people alive while also providing an incentive to murder, thus changing the dynamic from win-lose to mutually assured destruction, which in effect will bring about more peace. Such a system can be made autonomous without external interference, thus satisfying the goal of driving users to interact on a blockchain-based system.

The way this all starts is with a person, A, purchasing a “Deterrence Plan” (kill the person who kills me) for a yearly fee of X. To begin with, Person A (the person staking money in this insurance) will pay a yearly fee, via cryptocurrency to J1, a smart contract that distributes the digital currency into specific wallets. Once A has paid X, J1 sends 25% of the digital currency to the Originator’s account, while sending the other 75% into a vault, a multi-signature wallet which requires two keys. This vault can only be unlocked once both keys are submitted.

One would continue the process of staking annually. The tokens in the vault are the “bounty”, which this whole idea is based upon. The bounty is an amount for the head (elimination) of B, the guy who A chose to be the target of the contract. Once J2, a combination of a smart contract and a keyword script constantly scanning the internet, determines Event K (i.e. A is murdered or goes to jail) has happened, J2 then changes the public “bounty” status from inactive to active.

Once the “bounty” is set to active, C (anyone who is willing to wager) may start making “bets” on the date and location of B’s death. A bet in this instance is a combination of P (a prediction on the date and location of B’s death) and R (an amount of digital currency required to make a prediction). If J3 confirms that P was correct, then they unlock the vault, sending the amount within, Z, to C.

Part II: Mechanics of the System

Once A purchases a “Deterrence Plan” for a yearly fee of X, then A would pay this fee to J1, which programmatically allocates 25% to the Originator and 75% into the vault. Once J1 recognizes that it has been paid for a contract, it creates an “inactive bounty” (if J2 and J3 submit keys to J1, then J1 will unlock the vault & send tokens to the appropriate wallet) that is made public on the website. The bounty is worth X, with X being the amount of digital currency in the vault. Also, the bounty starts in a state of being inactive, meaning no one can place a bet on it. But if Event K happens, then J2 sets the status of the bounty on the website to active, meaning anyone can make a “bet” on the date and location of the death of B. What this means is that the longer one stakes within this system (the higher the amount in the vault), the more reason B has to stop Event K from happening. For example, if Pablo Escobar told the heads of the Cali Cartel that there is a 20 million dollar bounty to be set on each of their heads should he die of unnatural causes or go to jail, the Cali guys would likely try to keep Escobar alive and free so as to not have multiple, well-trained hitmen come after their heads. By using automated contracts with large monetary incentives, one can make B their ally in the game whether they like it or not. And if B does the same process, then a stalemate is reached between two potentially quarrelling parties. Neither can kill or harm the other without potentially dying themselves, creating peace through mutually assured destruction.

Now let’s say that Event K happened despite the “deterrence plan” A was paying. How would one collect this bounty without getting the metaphorical shaft from every government around the world? Well, that’s where the system detailed in Jim Bell’s paper is used. C would send P along with R to J3 via a two part “encrypted envelope.” R would be placed in the part of the envelope accessible by U1. J3 would then use U1 to transfer R to an “escrow” wallet. The wager remains in this wallet until J3 can confirm if P is true or not. P would be placed in the part of the envelope only decryptable by PK. If P could be confirmed true, then C would most likely send the PK and U2 to J3. If J3 uses PK to verify P is true, then J3 says that all existing P that have not been confirmed to be correct or incorrect, are now incorrect by default. All incorrect P have their correlating R taken from these “escrow” wallets and subsequently added to Z. Once J3 recognizes that all R’s that correlated to an incorrect P are now in the vault, J3 takes Z and sends it to C via an encrypted envelope. The envelope can only be unlocked using the U2 that C sent with the PK that revealed their correct P.

This paragraph will detail some important things that must happen. B must be identifiable. You can't say, "B is whomever kills me," because that isn't something that a program, J2, can verify. Instead, say "B is the judge who would oversee A's court case." Also, Event K must be more specific than "A dies" (though it doesn't have to, it is recommended). Event K should look like, "A dies from gang related activity," or " A gets arrested within a certain jurisdiction." Lastly, the publicly viewable bounty should always detail who and what Event K and B are, even in an inactive state. This would influence B to not want Event K happening. And even if B is not a unique person, people would avoid ever fitting the description of B, decreasing the likelihood of Event K ever happening. The system creates a game which provides incentive to buy more in order to coerce the real world actions of others.

Part III: Explaining Jx

Jx is the variable representation of the "incorruptible, omnipresent, external overseer[s]" that Dr. Virgil Griffith talks about in the aforementioned paper. They are essentially programs/smart contracts that enforce the rules of a given game. This section of my paper will detail how these programs work within the system.

J1 is the program that delegates which wallets the digital currency ends up in. It divides X into the 25% that goes to the originator wallet, and the 75% that goes to the vault (locked wallet). J1 then "locks'' the vault, a multi signature wallet requiring two keys. Digital currency can always be sent into the vault, but money can only leave the vault when the two keys are submitted. The first key requires J2's signature to confirm that the bounty is active. The second key requires J3's signature to confirm a correct P was made, only then being able to unlock the vault and the digital currency inside. The vault requires that J2's key is used before J3's key, otherwise the vault will remain locked.

J2 is the program that determines if Event K happens and determines who B is, while also setting the bounty to active. The way it is able to confirm Event K and B as true is by using a sort of observer program. J2 watches for certain keywords (Y1) to come up in online articles or records. For example, if you paid for Event K to be when you got arrested, then J2 would observe online police records and news articles worldwide for Y1, like the name of A, arrest, police, caught, etc. If J2 finds a certain number of Y1 within a certain amount of words, then J2 determines that Event K is true. If J2 determines that Event K is true, then J2 must determine B.

If B is already a specific, unique person (i.e. Richard Bruce Cheney or Nelson Rolihlahla Mandela), then J2 moves to the next step (basically skips this paragraph). If B is not a specific, unique person (i.e. The judge presiding over A's court case, or the governor of the area A was arrested in), then J2 does another keyword (Y2) identification program. If J2 finds enough Y2 to determine that a person meets the requirements needed to be B, then J2 moves onto the next step.

Once J2 can determine that Event K is true and it can determine who B is, it changes the state of the "bounty" from inactive to active, and names B. This "turns" the first key.

J3 is the program that determines if P is correct. The way J3 works is similar to J2, acting as an observer for certain keywords (Y3). J3 uses Y3 to look for obituaries, videos, and other online news/articles that could detail the exact location and date of B's death, looking for the earliest possible record. J3 determines from that search what a correct P should look like. When J3 determines that B is dead, the "bounty" on the website enters a state of "closed." That means no more guesses can be made, and that whatever guesses were sent prior to the exact time (to the minute) of B's death are in escrow until proven otherwise. There are two requirements for a correct P: the date guessed is correct, and the exact location (the supermarket on 37th street) must be within a 50 meter radius of the correct location. Once J3 uses PK to find that P is correct, all other R that are in "escrow" accounts are transferred to Z. Once that is done, J2 submits the second key, subsequently opening the vault. Once the vault is open, J1 sends Z to the address sent with the PK that unlocked the correct P.

Now there's a slight problem, what happens if no Event K's happen during A's lifetime? Well, that is something that J3 is preprogrammed to recognize. If A dies of causes not outlined by any Event K, then J3 unlocks the vault and sends 75% of Z to a person that A specified it be sent to in this event, with the other 25% going to the originator. That means there is an additional incentive to stake more. Because if the deterrence that the system provides results in Event K never happening, then A has created an untouchable and (hopefully) non taxable final will. So no matter what, the majority of X is being used to benefit A in some way.

Part IV: Money and Legality

Sets of Event K's and their corresponding B's are called contracts. The contract requires a, for example, USD $100k minimum in digital currency on a yearly basis per an Event K. A can assign as many B's to an Event K as they would like, but every B after the first costs an additional USD $50K minimum in digital currency. That means A can add deterrence to more than one outcome for more than one individual for additional fees. You basically incentivize people to buy more to increase deterrence. And despite each contract being separate, Z is pooled into the one account that belongs to A. This means that by preparing for more outcomes, one increases the potential bounty that will be placed on any number of B's, further increasing the likelihood that any B would not want any Event K to happen.

The way that this system is set up, with assistance from Jim Bell's model, it functions essentially as online gambling. C is betting R that P is correct against what the Z that A is betting that no one will guess right. It's like betting $5 that the roulette wheel will land on green against your friend who bet $3000 your ball won't land on green. If P is incorrect, R goes directly to the vault which houses Z. This means that all losing bets go to A, but A is still continuing to bet that no one will "guess" the correct date and location of B's death.

One of the upsides to using this model is that J1 and J3 only ever know that C existed and had a correct P. That means there is no way to definitively say C had anything to do with B's death, let alone identify whom C is to begin with. That means both the Originator and A would be of no use to the police in finding the murderer, while still doing nothing illegal themselves. And while gambling online is illegal in some parts of the world, it's far more legal than having a murder for hire website.

But now comes the question of how to deal with legal jurisdictions who may want such a system taken down? Well, if you own just a simple gambling website, where people can put up money to guess the date and location of people's deaths (and that's what you're actually doing), then no one can really touch you. But if the powers that be really wanted to throw the book at you, then you should use the system as deterrence for anyone getting anywhere near you. What all that means is that by using the system made by Jim Bell, anyone who wants to take down the system understands how the system works, meaning they would understand the great risk of death in even attempting such a feat.

Part V: The VIP Rank

Now, let's say you can use Charon's Obol to create a bounty and deter most B's from wanting Event K from happening. Well, the target of your bounty could use Charon to outbid you, making it so that even if Event K happens, B is completely safe. Well, to ensure that some individual A's will have precedent over their respective B's, bounties can now have ranks. We will use an arbitrary system of rank. Based on the amount of contracts and money spent with Charon, Variable A (the person creating a contract) can add further deterrence in the form of making their bounty a VIP Bounty (i.e. 10% more than a regular contract will be paid out).

A bounty being determined as a VIP is based on L (the amount of currency spent by A) multiplied by 0.25, then we divide Q (the number of inactive contracts A has made) by 2, then we add F (the number of active and completed contracts made by A) to the dividend of Q / 2. Lastly, we multiply the sum of ((Q / 2) + F) by (L x 2) to get V (the sum of our equation). So our equation is now: (L x 0.25) x ((Q / 2) + F) = V - And if V is greater than or equal to 20 million, then the account associated with A is now a VIP.

So what does this contrived rank have to do within Charon? Well, it means a successful guess on the date and location of B's death is worth more to C. In addition to C collecting their normal reward, they receive an additional 10% of that bounty from Charon itself. This means that the more A stakes, and the more contracts they create, the more valuable any of their contracts become. Also, VIP bounties will be put above regular bounties, meaning that the more rich and powerful one is, the more deterrence they have. To Variable C, this means a larger payout than normal, which means more incentive to correctly "guess" the date and location of B's death. To Variable B, this VIP status means that they can almost always be outbid by the VIP. If they can't win using Charon, then they should prevent Event K from ever happening.

Summary

Based on the ideas and items detailed in this paper, I propose that one can make a system which incentivizes the use of the blockchain to ensure certain individual's survival, while also using it to incentivize the deaths of other individuals. And to increase the effectiveness of the "threats" this system creates, VIP's can increase the amount their bounty is worth. Lastly, by using an impartial and incorruptible judge in the form of smart contracts and additional programs, one can manipulate the actions of specific people by simply paying for these contracts to exist.

The larger ramifications of such a system would mean that eventually, every person alive would have to adhere to certain behavior or risk death. That means such a system could be used to create an environment that would bring about world peace through the threat of mutually assured destruction.

Flow Chart

[

Charon's Obol

1680×1316 218 KB

](https://ethresear.ch/uploads/default/original/2X/7/79477ed0cd1c13486960fc8826b975a069dc2ed8.png)

Flow Chart Legend

Blue Line: Flow of money

Red Line: Flow of information

Yellow Line: Key insertion

Black Line: Flow of Non-blockchain actions

Legend

Here's a legend so you can keep track of which variables represent which things

A: Initial person buying insurance

B: The target of the bounty

C: Person who is trying to claim Z

J1: The program/smart contract that handles the distribution of X, and “creates” bounty

J2: The program/smart contract that determines if a bounty is active

J3: The program/smart contract that determines if P is correct, and gives Z to C

X: The amount which A payed for the deterrence plan

Z: The 75% of X that remains in the vault, the bounty on B

Event K: The bounty trigger event

P: A prediction of the location and day which B dies

R: The amount C is willing to wager that P is correct

Y1: Keywords that J2 uses to determine if Event K happened

Y2: Keywords J2 uses to determine who B is

Y3: Keywords that J3 uses to determine what the correct P is

PK: Private key unique to C that is used to confirm if P is correct

U1: Public key used by J3 to collect R

U2: Public key by C to collect Z

L: Total amount of currency spent by A

Q: Number of inactive contracts made by A

F: Number of completed and active contracts made by A

V: Sum of the “VIP Equation”

Bibliography

- “Assassination Politics” by Jim Bell (https://cryptome.org/ap.htm)
- “Ethereum is game-changing technology, literally.” by Virgil Griffith (Ethereum is game-changing technology, literally. | by Virgil Griffith | Medium)