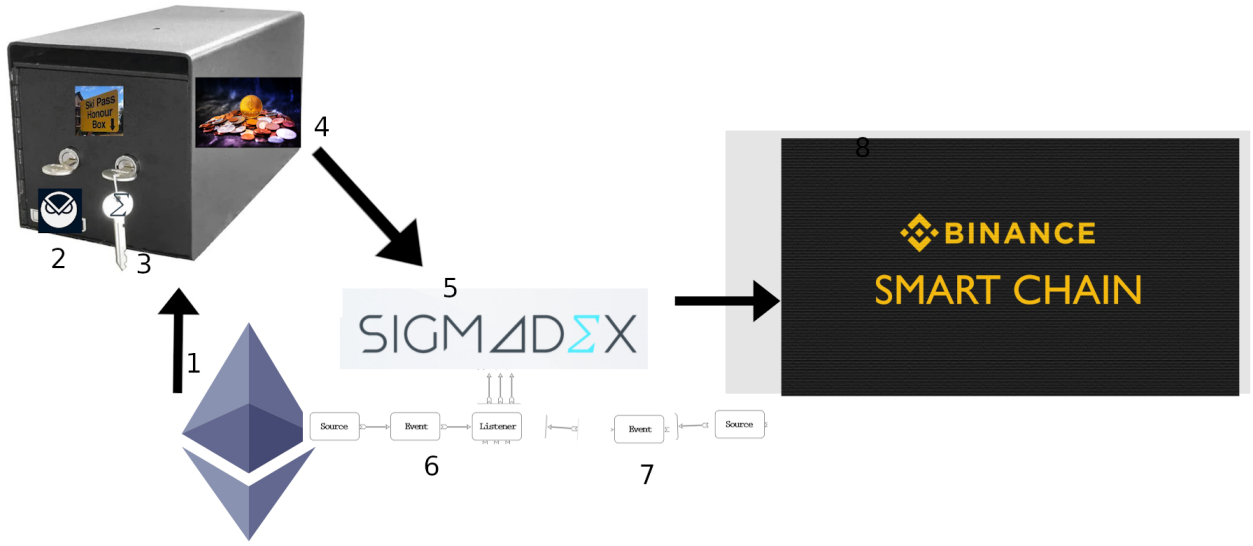

Figure 1: Basic Network Diagram. A factory contract based on Gnosis-safe is placed on the Ethereum Blockchain that produces an honourbox at a users request. One key of this bi-signature wallet is kept by the user, the other given to sigmadex. The Sigmadex engine listens for a user depositing their crypto in the honourbox, upon which it mints pegged Tokens on the sigmadex platforms built initially on the binance smart chain. Prior to each state transformation, sigmadex checks the state of the honourbox before allowing or disallowing an action within the platform. Since a user can always withdrawal their ethereum assets, they are safe from bridger operators

THE HONOURBOX BRIDGING ARCHITECTURE

A PREPRINT

Taylor Hulsmans*
Blockchain Developer
Sigmadex
Calgary, Ab
taylor@danihelgroup.com

May 25, 2021

ABSTRACT

A novel blockchain bridging architecture is modelled and discussed. Its motivation derives from the desire to give the bridge crosser a security guarantee against centralized and decentralized bridge operators. A user deposits their crypto in a bi-signature wallet contract called an honourbox, by which both the user and Sigmadex can unilaterally withdrawal from, but not without losing the box in the case of the user, and loss of integrity for Sigmadex. Bridge integrity is secured by coupling the bridge to the use-case (in our case a swap of two cryptocurrencies) and structuring a carrot and stick policy the induces cooperation between participants rationally through the repeated prisoners dilemma. This policy materializes as an honour point leveling system that enables higher volume trades and increases the value of their honourbox that can be confiscated in the event of inappropriately removing

*Blockchain Dev, Sigmadex

their funds from the box. Ideas such as the max risk free swap, probabilistically likely swaps, and perpetuity considerations are developed. Additional policies for honour acquisition, such as self KYC and sinking transaction costs into cosmetic upgrades are discussed alongside its similarity to Wampum.

Figure 2: An Honourbox system supports trail maintenance at 100 Mile House, British Columbia, Canada

Keywords Blockchain, Bridging, Decentralized Exchange, Ethereum, Binance Smart Chain

1 Introduction

Solutions to the challenge of blockchain interoperability are a current open question in the DLT community. While decentralized solutions have been attempted utilizing PoA or PoS validator networks, at the end of the day, these solutions are economically bounded over how much is staked or bonded by validators. In the world where there is always a bigger whale, even these decentralized architectures must resort to centralized strategies like enable/disable bridge from a superaccount, or implement less than savoury smart contract upgrade architectures to fully close the system. Indeed, in my own review of the space in general, and especially in respect to low collateralization environments, the statement "We formalize the underlying research problem and show that CCC (cross chain communication) is impossible without a trusted third party, contrary to common beliefs in the blockchain community".[1] is well appreciated.

If one than assumed, by the prior source, that trust-less, decentralized bridges are impossible in nature, than the solution to blockchain interoperability must be approached from a different perspective. How would one go about providing a guarantee that a users crypto cannot be stranded, while at the same time providing a guarantee of the bridges accounting integrity? The solution provided herein, the honour box bridging architecture, allows a user to be 100 percent certain they can get their crypto out in case of emergency, as it really never leaves his custody, while actions on the other side are subject to a punishment/reward system that constrains moves onthe DEX by the repeated prisoners dilemma. The goal exposed to the user is simple, self stake tokens in an honour box, receive tokens on the other chain, and use Sigmadex. If the user chooses to engage in bad behaviour, they are punished by the seizure of ones honourbox to

be placed on the secondary market for a process called redemption, by which another user can payout that who got scammed, plus a fee, to start with that honourbox, instead of from scatch. We will see there are a number of ways to increase the value of ones honourbox beyond faithful platform use, such as self KYC, sinking gas fees into cosmetic upgrades, and much more.

The structure of the following paper is as follows, we begin with a review of the repeated prisoners dilemma to understand how even rational players will choose cooperate if they believe the other user is likely enough to continue using Sigmadex in the future. We than apply this model upon the decision to honour or dishonour a swap agreement on sigmadex. We than discuss the risk-free max-swap amount as the point where the critical probability is 0, the area where it is functionally unlikely 0-5, than the areas where a user will need to use their own judgement based on the other users profile to determine the risk, and than finally when there is so much reputation that a user believes they will operate in perpetuity. Figure 1.

2 The Repeated Prisoners Dilemma

The special glue that holds this architecture together is predicated on the idea that rational actors facing the repeated prisoners dilemma game will pick the pareto-efficient collusion strategy if they sufficiently believe the other party will play the game again given the payoffs. This uncertainty over if/when a user will dishonour resolves the paradox of backward induction and sets up "the circumstances where credible threats and promises to secure a particular strategy, such as cooperation in the prisoners' dilemma, can be made.[2]

Table 1: The Generalized Prisoners Dilemma

		Player Y	
		A	B
Player X	A	(a, a)	(b, c)
	B	(c, b)	(d, d)

Where c > a > d > b.

If the probability that the game will be played more than one time is P, and more than n times is p_n, than the expected payoff of cooperating with his counter party is

$$EPO_{coop} = a + aP + aP_2 + aP_3 + ...aP_n = \sum_{n=0}^{\infty} aP_n = \frac{a}{1-P}$$

and the expected payoff of defecting against his counter party is

$$EPO_{defect} = c + dP + dP_2 + dP_3 + ...dP_n = c + \sum_{n=0}^{\infty} dP_n = c + \frac{dP}{1-P}$$

than we can define a critical probability threshold where

$$EPO_{coop} > EPO_{defect}$$

resulting in

$$P > \frac{a-c}{d-c}$$

In other terms, If a player believes the probability that his counter party will use sigmadex at least once more after him is greater than $\frac{a-c}{d-c}$, than cooperate is not only the pareto-efficient outcome, but also the nash dominant. When P becomes so great as is practical to assume your counter party will play forever, than we can substitute P for F where

$$F = \frac{1}{1+r}$$

$$F > \frac{a-c}{d-c}$$

where F is denoted the discount rate and r the annualized rate of return of the asset

2.1 Applying to a swap agreement

A most basic function of Sigmadex will be in the implementation of swaps between parties. Using the honourbox architecture, we can model the game as a prisoners dilemma between honouring and dishonouring the swap. Exogenous variables for transaction costs on both networks, the rate of return of the asset are added, the endogenous variable for swap volume is included. Parameters that characterize the swap utility and honour utility are included. Critically, a punishment strategy is implemented, that if a player dishonours their commitment, Sigmadex can seize the honourbox from the user, and place it into a separate marketplace. Redemption allows for the refunding of whomever got scammed, and allows a new player to not have to start from the bottom by buying this box. This allows sigmadex to generate efficient estimates on the marginal price of honour and a boxes particular value. Mathematically, the game is of the character.

Table 2: To Honour or Dishonour a Swap Agreement

		Player Y	
		$HonourSwap$	$DishonourSwap$
2*Player X	$HonourSwap$	(a, a)	(b, c)
	$DishonourSwap$	(c, b)	(d, d)

Table 3: Payoffs

Payoff	Equation	Comments
a	CV + σ + κ - tx_{bsc}	Cooperative payout
b	-tx_{bsc}	Price of getting scammed
c	2*CV + σ - tx_{eth} - tx_{bsc} - BV	Scamming
d	CV - tx_{eth} - tx_{bsc} - BV	Both attempting to scam

Table 4: Values

Symbol	Value	Explanation
CV	Coin Value	Value of token being swapped
σ	swap Value	subjective, assumed >= tx_{bsc}
κ	honour Value	priced by honourbox repo market
tx_{bsc}	tx cost bsc	Transaction cost of swap on BSC
tx_{eth}	tx cost eth	cost of removing ETH from lockbox
BV	Box Value	priced by honourbox repo market

From theses values than, a critical P can be characterized for comparison

$$P^* = \frac{\kappa + tx_{eth} - CV + BV}{-\sigma - CV}$$

Given the cost of an ethereum transfer and the economic resale value of a box, it is reasonable to characterize the max risk free swap. Before this value, the game is in fact not even a prisoners dilemma, and honouring the swap is the pareto-efficient nash equilibria. To find the max risk free swap we find the CV where P = 0

$$CV = \kappa + tx_{eth} + BV$$

After this swap range, we begin receiving positive critical values of P, When P reaches one even if the user was gauranteed to play again, defection is higher valued. This is reached in the limit

$$\lim_{CV \to \infty} \frac{\kappa + tx_{eth} - CV + BV}{-\sigma - CV} = 1$$

$$\frac{\partial P}{\partial CV} = \frac{\sigma + \kappa + tx_{eth} + BV}{(-\sigma - CV)^2}$$

In order for a user to increase the volume they can swap, a user can look to increasing the value of their box in several ways. Among them being to accumulate honour points κ through faithful use of the platform, cosmetically upgrade

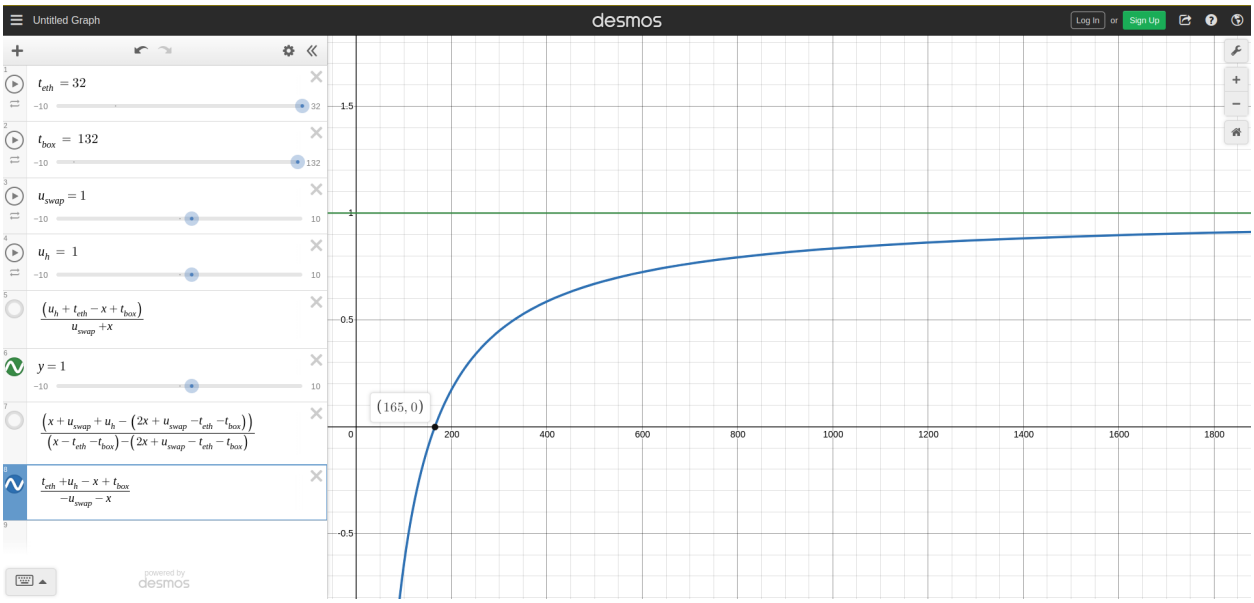

Figure 3: visualizing the critical P value as the swap value increases, here we can not the max risk free swap where the y-axis is zero, and the curve that characterizes how the critical value needed grows as the swap value increases

your honourbox, volunteer for KYC (lost on new owner), among others. The Key is that every honour box is an NFT that competes for prestige and credibility that grows with the users good behaviour, opening up more risk and more prestige. The value of honour and a users box is inferred from the market price of dishonoured boxes.

When a user commits a dishonour, Sigmadex has the right and obligation to remove the box from the possession of the counter party. Sigmadex than places it on the open market for NFT honourboxes. Individuals who would rather pay to win than start from scratch can purchase these boxes by refunding the person who got scammed, reclaiming the box and its honour. This process is known as redemption. Since it is a floating price, mostly based on intangibles designed to help a user inform their own opinion on another users likelyhood to use the platform again. Sigmadex bases its value on sunk costs of production- the gas cost of creating the box, cosmetically upgrading the box explicitly, and infers the value of honour by comparing the box to another with similar honour on market. Conservative estimators and linear additions to honour form a basic model to begin with, but as the platform grows its entirely reasonable to introduce non-linear honour rewards, and begin implementing machine learning models built from the behavioural economics of the prisoners dilemma to gather more reliable estimators for the Box Value and honour points. Increasing ones Box Value than decreases the required critical P by the equation

$$\frac{\partial P}{\partial BV} = -\frac{1}{(-\sigma + CV)}$$

Figure 3. The idea behind honourbox upgrading is effectively similar to how Native American Peoples utilized Wampum[3] as a form of currency, honour, authority, trustworthiness and much else concerning the valuation and forthrightness of their tribe. Hopefully, with the power of 3d, users will be able to create beautiful and meaningful wampums to help empower higher trust levels between participants, allowing higher volume trades with greater critical P values.

2.2 Volatility Considerations: Managing the Asymmetric Prisoners Dilemma

The framework described above is useful when considering the relative value of the coins remains roughly equal over the time staked. However, this will almost never be the case save stablecoins. The series of games that emerge coincide with 25 social dilemma games[4], and more explicitly, the alibi games[4]. The following section describes the systems by which the game returns to symmetry.

The game than, can be decomposed into an asymmetric and symmetric component

Where

$$CV_2 = CV_1 - x = CV_1 - y$$

Table 5: Introducing Asymmetric coin values

		Player 2	
		$HonourSwap$	$DishonourSwap$
Player 1	$HonourSwap$	(a_1, a_2)	(b, c)
	$DishonourSwap$	(c, b)	(d_1, d_2)

Table 6: Payoffs

Payoff	Equation	Comments
a_1	CV_2 + σ + κ - tx_{bsc}	Cooperative payout
a_2	CV_1 + σ + κ - tx_{bsc}	Cooperative payout
b	-tx_{bsc}	Price of getting scammed
c	CV_1 + CV_2 + σ - tx_{eth} - tx_{bsc} - BV	Scamming
d_1	CV_1 - tx_{eth} - tx_{bsc} - BV	Both attempting to scam
d_2	CV_2 - tx_{eth} - tx_{bsc} - BV	Both attempting to scam

Table 7: Values

Symbol	Value	Explanation
CV_1	Coin Value of player ones stake	Value of token being swapped USD
CV_2	Coin Value of player twos stake	Value of token being swapped USD
σ	swap Value	subjective, assumed >= tx_{bsc}
κ	honour Value	priced by honourbox repo market
tx_{bsc}	tx cost bsc	Transaction cost of swap on BSC
tx_{eth}	tx cost eth	cost of removing ETH from lockbox
BV	Box Value	priced by honourbox repo market

Table 8: Asymmetric component

		Player 2	
		$HonourSwap$	$DishonourSwap$
Player 1	$HonourSwap$	$(0, x)$	$(0, 0)$
	$DishonourSwap$	$(0, 0)$	$(y, 0)$

Table 9: Payoffs

Payoff	Equation	Comments
x	CV_1 + σ + κ - tx_{bsc} - a_1	increased incentive to coop for p2, holder of the coin that decreased in value
y	CV_1 - tx_{eth} + tx_{bsc} - BV - d_2	increased incentive to deviate for p1, holder of the coin that increased in value

Table 10: Symmetric component

		Player Y	
		$HonourSwap$	$DishonourSwap$
2*Player X	$HonourSwap$	(i_1, i_2)	(j, k)
	$DishonourSwap$	(k, j)	(l_1, l_2)

As sigmadex in nature operates as a continuous, simultaneous game, it is to be expected that there will exist an arbitrary amount of time between a swap and a moment when a user offloads their crypto. As such, the relative value of the tokens changing after a swap will incentivize the person holding the appreciated crypto to deviate, while incentivizing the holder of the depreciated crypto to cooperate. To manage this affect, two systems are implemented. The first being the voluntary timelocking of tokens within ones honourbox, and the second being an daily honour incentive for continuing to hold appreciated crypto. One would expect that marginal value of honour to be low during the initial stages of sigmadex due to lack of demand, as such timelocking is unboxed first.

When a user deposits crypto into their honourbox, an option will be provided to enter a date alongside it that cryptographically prevents the user from withdrawing that crypto until an end date. It is worth mentioning that

Table 11: Symmetric Payoffs

Payoff	Equation	Comments
i_1	CV_2 + σ + κ - tx_{bsc}	Cooperative payout
i_2	CV_1 + σ + κ - tx_{bsc} - x	Cooperative payout
j	-tx_{bsc}	Price of getting scammed
k	CV_1 + CV_2 + σ - tx_{eth} - tx_{bsc} - BV	Scamming
l_1	CV_1 - tx_{eth} - tx_{bsc} - BV - y	Both attempting to scam
l_2	CV_2 - tx_{eth} - tx_{bsc} - BV	Both attempting to scam

sigmadex will still be able to withdraw in the event of offboarding the swapped assets. In the economic model, this translates into decreasing the payoffs of defection by limiting the amount of coins that can be scammed away, an re introducing symettry by automatically offboarding the minimum required amount of the counter parties crypto to player 1. Referencing the asymmetric component we can determine the concept of minimum required timelock $CV_{1timelock}$ for the coin appreciating in value. To balance the incentives under timelock, in the event the counter party requests an offboard of player 1'c appreciated crypto thats timelocked, sigmadex automatically offboards the equivalent value of player twos stake to the user.

Table 12: Timelocking the appreciated coin

		Player 2	
		$HonourSwap$	$DishonourSwap$
Player 1	$HonourSwap$	(a_1, a_2)	(b, c_2)
	$DishonourSwap$	(c_1, b)	(d_1, d_2)

Table 13: Payoffs

Payoff	Equation	Comments
a_1	CV_2 + σ + κ - tx_{bsc}	Cooperative payout
a_2	CV_1 + σ + κ - tx_{bsc}	Cooperative payout
b	-tx_{bsc}	Price of getting scammed
c_1	CV_1 - $CV_{1timelock}$ + CV_2 + σ - tx_{eth} - tx_{bsc} - BV	Scamming
c_2	CV_1 + CV_2 - $CV_{2-1timelock}$ + σ - tx_{eth} - tx_{bsc} - BV	Scamming
d_1	CV_1 - $CV_{1timelock}$ - tx_{eth} - tx_{bsc} - BV	Both attempting to scam
d_2	CV_2 - $CV_{2-1timelock}$ - tx_{eth} - tx_{bsc} - BV	Both attempting to scam

Table 14: Values

Symbol	Value	Explanation
CV_1	Coin Value of player ones stake	Value of token being swapped USD
CV_2	Coin Value of player twos stake	Value of token being swapped USD
$CV_{1timelock}$	Coin Value of player ones timelock	amount inaccessible to p1
$CV_{2-1timelock}$	Coin Value of player ones timelock in p2 crypto	amount automatically swapped to p1 if p2 offboards
σ	swap Value	subjective, assumed >= tx_{bsc}
κ	honour Value	priced by honourbox repo market
tx_{bsc}	tx cost bsc	Transaction cost of swap on BSC
tx_{eth}	tx cost eth	cost of removing ETH from lockbox
BV	Box Value	priced by honourbox repo market

Without rehashing the equations, it is sufficient to comprehend that the the timelocking of crypto reduces the payoffs of defecting strategies, offering a sort of insurance that can aid in higher volume swaps at the cost of the freedom to be able to withdrawal ones crypto at anytime and the possibility of having a portion of ones paper gains hashed onto ethereum if ones counterparty attempts to defect. On the offboarding end, Sigmadex treats $CV_{1timelock}$ and $CV_{2-1timelock}$ as maximum required amounts, and will minimize the amount required to timelock needed to balance CV_2 and CV_1, even going so far as to remove a portion of player1s time locked funds and giving it back to him, to provide PD game symettry in the wave of token volatility

$$CV_2 = CV_1 - x = CV_1 - y$$

Return back to this function, a secondary system for managing token volatility comes into play when sigmadex reaches enough usage that the market for dishonoured boxes is active enough to return the shadow price of a point of honour. A user holding the appreciated crypto is than awarded daily with additional honour points per the marginal price of honour to quench the temptation of defection. This amount would be equal to x and y in the above equation.

2.3 Managing the Asymmetry of Box Value

3 Conclusion

A Novel Bridging Architecture that brings a degree of control back to the user given the impossibility of a bridges existence without a central 3rd party is presented. The solution embraces the trust of rational actors operating in a repeated prisoners dilemma game. Tokens are never removed from the custody of the user crossing the bridge, solving the centralization problem. Guarantees of the stakes legitimacy are kept with a carrot and stick strategy that promises more network utility for good behaviour, and loss of network utility with bad. The idea of a minimum-swap amount is disfavoured for the idea of max risk-free swap, and probabilistically favoured swaps. A user relies on various forms of trust signals to determine if they think the probability of their counterparty using Sigmadex again to compare against the critical P value calculated by the algorithm. Token Volatility is managed by teasing apart the asymmetric and symmetric component of the game, and offering tools and policies that re-balance the game, such as volunteer timelocking of tokens, and the introduction of additional honour incentives for holders of appreciated assets.

References

[1] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, William Knottenbelt" (2021) *SoK: Communication Across Distributed Ledgers*, Financial Cryptography and Data Security 2021,
https://eprint.iacr.org/2019/1128.pdf

[2] Fiona Carmichael(2004) *A Guide to Game Theory*, Prentice Hall, (203-216).

[3] Wampum: Canadian Encyclopedia
https://www.thecanadianencyclopedia.ca/en/article/wampum

[4] Robinson, David and Goforth, David (2005) *The Topology of the 2x2 games: A New Periodic Table*
https://www.researchgate.net/publication/266995029_The_Topology_of_the_2x2_games_A_New_Periodic_Table

[5] Robinson, David and Goforth, David (2004) *Alibi games: the Asymmetric Prisoner's Dilemmas*
https://www.researchgate.net/publication/265796653_Alibi_games_the_Asymmetric_Prisoner's_Dilemmas