CONTINGENCY

The World's First Decentralized, Trustless Gambling Network Based on Smart Contracts. Contingency is an upcoming decentralized gambling network that will allow individuals to:

a) Bet ether or any ERC20 standard token.

b) Become a 'banker' and have other individuals try their luck against them.

c) Create their own games for others to play on.

Unlike traditional online casino platforms, Players and bankers are always in control of their own cryptocurrency, and never have to send them to the Contingency founders. This prevents many forms of attack that have led to loss in the past with traditional platforms

Trustless

Traditional models hold player funds inside online wallets or bank accounts controlled by the operators, this makes online casinos a huge target for hack attempts or malicious conduct by employees. Players and bankers ether and/or tokens are never held by the Contingency operators, but are instead stored in a smart contract hosted on the Ethereum blockchain. Individuals therefore have direct, 24/7 access to their funds at all times. If the Contingency operators were hackers or decided to become malicious, all user funds will be safe.

Automated

Players may wager on using the Contingency smart contract, in which their bet is submitted and available for a banker to process. Once bankers have obtained the required CTY and deposited ether and/or another token. They can then run the banker software on their PC and have the entire process automated. Bets received by other players will be computed and resolved automatically and instantly, and then broadcast to the Ethereum network.

Market and Opportunity

Online crypto-token gambling is an ever increasing market. Satoshi Dice launched on Bitcoin in 2012, marking the first major Provably Fair crypto gambling platform. Since then, demand has grown and driven the need for more fair, cheaper, and trustworthy gambling networks. In the last year alone, almost 10 billion bets have been placed across bitcoin casinos. With 1,364,101 BTC wagered or $850 million USD.

Casino	Bets	Wagered
Primedice	6.14 billion	556,108 BTC
bustabit	129.78 million	323,834 BTC
BetKing	81.78 million	122,817 BTC
SatoshiDice	334.27 million	64,386 BTC
BetterBets	293.21 million	41,411 BTC
BitDice	12.25 million	37,729 BTC

Source: https://thebitcoinstrip.com/stats/

With the release of Ethereum, and crypto-tokens becoming ever-more in demand, this number is expected to drastically rise. Contingency aims to mark the way for a new breed of gambling platforms. Where zero downtime is experienced, zero thefts will occur, and zero trust is required to participate and feel safe.

The Solution

Contingency will be the world's first truly decentralized, trustless gambling network. Contingency will never hold a user's funds, and never process a user's bet, instead, we will be creating a network that allows gamblers to automatically find online bankers, and instantly wager against them. With the usage of Ethereum smart-contracts, users will be able to directly wager their ether and ERC20 based tokens without any middlemen such as a bank or casino operator. All with the knowledge that their funds are not being held by a third party to be subject to the risk of hacks, theft, or misconduct. The decentralized nature of Ethereum will ensure that all steps of the process are transparent and fair, and unmanipulated by any third party.

Future Vision

Contingency plans to become to biggest gambling network in the crypto space. We plan to set a new standard in the way that fair and trustless gambling games can be created, and to greatly reduce the amount of hacks and theft in the industry.

Using Contingency

Wagering Anyone can play on Contingency without borders or restrictions. CTY tokens are not required to wager bets. Contingency supports ether as well as any ERC20 based token. This includes Augur (REP), Plutons (PLU) and Contingency (CTY) tokens and is future-proof for tokens that are yet to exist.

Bets are placed using the following function: function bet(address token, uint amount, uint lessThan, bytes32 seed);

Players create a bet by calling the bet() function on the Contingency smart contract. This must include the token' they wish to bet (or 0x0 if they wish to bet ether), the amount' the wish to wager, the lessThan' target they predict to hit (out of 64000), and a random seed' which ensures their bet outcome cannot be predicted by the banker.

To place a 50/50 bet of 1000 wei, the player would call bet(0x0, 1000, 32000, Math.random());

A user-friendly interface will be created so that anyone can play just like they would on a traditional online casino, and not have to use the above command.

Creating Games

Any individual can create Contingency games. Games are created using Solidity and referencing the Contingency contract.

As of writing this whitepaper, games are fixed to a 1% banker-edge and must be a simple dice-roll. We plan to upgrade this to allow bigger (but not smaller) banker-edges and a variety of roll types such as array shuffling (Eg. For card games similar to BlackJack).

Below is a simple untested game that can be created:

```
1  contract ContingencyGame {
2      // A simple game that allows betting with ETH or any Ethereum
           standard token
3      address contingencyAddress;
4      struct Bet {
5          uint betID;
6          address token;
7      }
8      mapping(address => Bet) bets;
9
10     function GameToken(address cAddress) {
11         contingencyAddress = cAddress;
12     }
13
14     function bet(address token, uint amount, uint lessThan, bytes32 seed
           ) {
15         if (bets[msg.sender].betID != 0) {
16             // Existing bet
17             if (Contingency(contingencyAddress).getStatus(bets[msg.
                   sender].token,
18                     bets[msg.sender].betID) == 0) {
19                 throw; // Bet still pending
20             }
21         }
22         if (token == 0) {
23             amount = msg.value;
24         } else {
25             if (!Token(token).transferFrom(msg.sender, this, amount))
                   throw;
26         }
```

```
27          uint betID = Contingency ( contingencyAddress ). betToken ( token ,
                amount ,
28               lessThan , seed );
29          if ( betID == 0) throw ;
30          Bet bet = bets [ msg . sender ];
31          bet . betID = betID ;
32          bet . token = token ;
33      }
34
35      function claimWin () {
36          Bet bet = bets [ msg . sender ];
37          uint winnings = Contingency ( contingencyAddress ). claimWinToken (
                bet . token ,
38               bet . betID );
39          if ( winnings == 0) throw ;
40          if ( bet . token == 0) {
41              if (! msg . sender . send ( winnings )) throw ;
42          } else {
43              if (! Token ( bet . token ). transfer ( msg . sender , winnings )) throw ;
44          }
45          delete bets [ msg . sender ];
46      }
47 }
```

Being the Bank

Contingency's most unique feature, is the ability to be able to be the bank and accept players wagers. Once an individual has acquired CTY tokens (Either via the pre-re-salesale or an exchange afterwards), they can participate in the pool of bankers. Individuals in this pool will be able to play as the house when a wager is placed.

Almost all casino games in the world have what is called a 'house-edge' (Called a banker-edge in Contingency). This is a percentage that the odds are swayed in the house's (or bankers) favour (1% on Contingency). Over enough time, the banker will always profit due to the law of large numbers.

CTY Token

The Contingency Token (CTY) is an Ethereum ERC20 standard token. CTY will allow individuals to store ether as well as any ERC20 token in the smart contract so that it can be wagered against by players. This includes (but is not limited to) Plutons (PLU) and Augur Tokens (REP). They will effectively be acting as a casino operator and obtaining profits through the form of a house edge.

When a player goes to place a wager, a banker is selected by the Contingency smart contract that has enough balance to cover their bet's winnings.

The banker is selected by their amount of CTY holdings divided by the total amount of CTY currently being used by bankers.

BANKER_SHARE = BANKER_CTY / TOTAL_USED_CTY

A random number, generated by the player's seed and current block hash is used to determine which banker is selected using this weighted scale. Bankers with more CTY tokens have a higher chance of being selected, and thus will be able to process more bets, and earn more ether or tokens.

Pre-sale

The Contingency Token will only be created during a one-time pre-sale beginning February 1st, 2017 and completing February 28th, 2017. CTY tokens are required in order to provide Ether or any other Ethereum based Token to be wagered against into the network. They provide a way of selecting the banker that a player's wager will be bet against. The more CTY you own, the more your position will be wagered against, and the more you will (accounting for volatility) earn. Banker tokens will be released on a timeline starting from 170 CNY = 1 eth during the first hour of the sale, down to 100 CTY = 1 ETH on the last days.
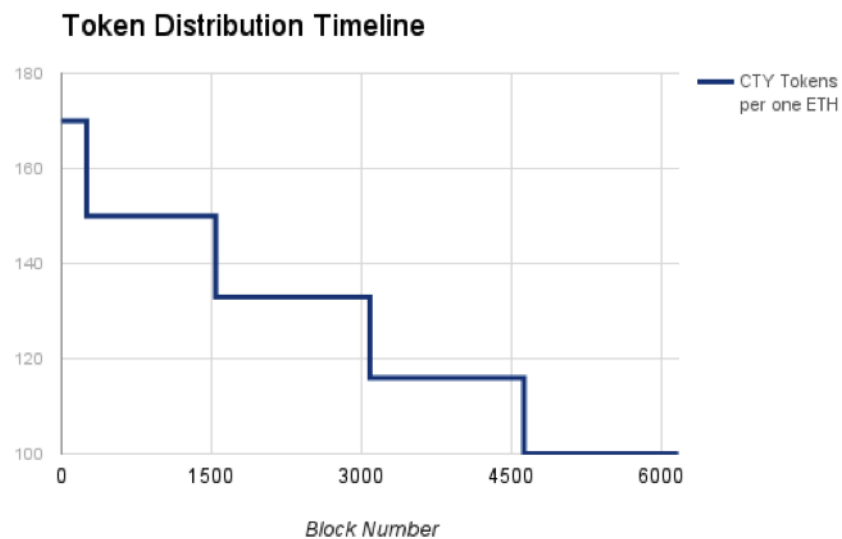
At the end of the sale, the founding team will receive a 10% allocation of CTY. These coins will be locked from being transferred for one year to act as a long term incentive for the team.

'Ain't broke, don't fix': To ensure the pre-sale goes smoothly, we are using a modified version of the firstblood.io pre-sale smart-contract. This contract was tested and executed well during the sale.

How Contingency solves the Blockchain RNG (Random Number Generator) problem

Tradition online betting platforms use server-based software to provide RNGs. Many online cryptocurrency platforms also provide what's known as provably fair number generation.

Both these methods rely on a central server to provide the generation, and cannot easily be adapted in a decentralized manner. When generating random numbers in a smart contract, outcomes can be manipulated by block miners or even individual users, depending on how the contract is set up.

Contingency solves this problem by not using random numbers at all. Instead the outcome of a wager is determined by the hash of a seed provided by both the player and banker.

A CTY holder first provides a hashed version of their secret, preventing them from providing a different secret later on. The player then places their bet and provides a seed.

The banker must then provide their secret which hashes correctly to their hashed secret. The number provided to the bet is the hash of the player seed and banker secret. All betting on Contingency is peer-to-peer. One player vs one banker.

Step by step wagering process:

– Banker provides **sha256(BANKER_SECRET)**

– Player provides **PLAYER_SEED**

– Banker completes the by generating the result using
   SHA256(PLAYER_SEED, BANKER_SECRET)

Accessing Contingency

Contingency.io will provide an easy-to-use front end that interacts with the Contingency smart contracts. This can be done via Ethereum clients such as Mist or MetaMask. Individuals will not need any programming knowledge in order to interface with Contingency.

Since BANKER is a completely decentralized platform built on smart contracts, should the platform ever go down, individuals will be able to interface with the network directly using an Ethereum client, or by using a third party front-end interface. No funds will ever be lost due to Contingency.io shutting down.

Timeline

December 2016: Announcement & White Paper release.

February 2017: Pre-sale

March 2017: In-house testing and programming

July 2017: Alpha testing for CTY holders.

September 2017: Public beta.

Pre-sale Breakdown

50% - Smart contract creation, tech design and UI

5% - Legal

10% - Security testing

5% - Bug Bounties

20% - Marketing

5% - General administrative

5% - Misc and reserves

Disclaimer

Contingency is not a gambling platform and does not process wagers. Contingency never holds the funds of any user and does not determine the outcome of any wager placed, and thus, cannot be held liable for any lost bet or winnings due to CTY token holders or operators. Contingency allows players to be matched up against other individual bankers. Users should check with their jurisdiction if using the service is legal for them. Purchas-

ing CTY is NOT an investment. CTY tokens allow a user to provide their own ether or ERC20 tokens to be wagered against by other players directly, and is used to determine the chance of being chosen by the smart contract.

Contingency Token, or 'CTY', is a cryptographic token used by the Contingency network.

CTY is not a cryptocurrency.

At the time of this writing, CTY (i) cannot be exchanged for goods or services, (ii) has no known uses outside the Contingency network, and (iii) cannot be traded on any known exchanges.

CTY is not an investment.

There is no guarantee - indeed there is no reason to believe - that the CTY you purchase will increase in value. It may - and probably will at some point - decrease in value. Those who do not actually use their CTY honestly and fairly will lose their CTY to those who do.

CTY is not evidence of ownership or right to control.

Controlling CTY does not grant its controller ownership or equity in Contingency, or the Contingency network. CTY does not grant any right to participate in the control the direction or decision making of Contingency or the Contingency Network.

1) Risk of Losing Access to CTY Due to Loss of Credentials

The purchaser's CTY may be associated with an Contingency account until they are distributed to the purchaser. The Contingency account can only be accessed with login credentials selected by the purchaser. The loss of these credentials will result in the loss of CTY. Best practices dictate that purchasers safely store credentials in one or more backup locations geographically separated from the working location.

2) Risks Associated with the Ethereum Protocol

CTY and the Contingency network are based upon the Ethereum protocol. As such, any malfunction, unintended function or unexpected functioning of the Ethereum protocol

may cause the Contingency network or CTY to malfunction or function in an unexpected or unintended manner. Ether, the native unit of account of the Ethereum Protocol may itself lose value in ways similar to CTY, and also other ways. More information about the Ethereum protocol is available at http://www.Ethereum.org.

3) Risks Associated with Purchaser Credentials

Any third party that gains access to the purchaser's login credentials or private keys may be able to dispose of the purchaser's CTY. To minimize this risk, the purchaser should guard against unauthorized access to their electronic devices.

4) Risk of Unfavorable Regulatory Action in One or More Jurisdictions

Blockchain technologies have been the subject of scrutiny by various regulatory bodies around the world. The functioning of the Contingency network and CTY could be impacted by one or more regulatory inquiries or actions, including but not limited to restrictions on the use or possession of digital tokens like CTY, which could impede or limit the development of the Contingency network.

5) Risk of Alternative, Unofficial Contingency Networks

Following the pre-sale and the development of the initial version of the CTY platform, it is possible that alternative networks could be established, which utilize the same open source code and open source protocol underlying the Contingency network. The official Contingency network may compete with these alternative, unofficial CTY-based networks, which could potentially negatively impact the Contingency network and CTY.

6) Risk of Insufficient Interest in the Contingency Network or Distributed Applications

It is possible that the Contingency network will not be used by a large number of businesses, individuals, and other organizations and that there will be limited public interest in the creation and development of distributed applications. Such a lack of interest could impact the development of the Contingency network and therefore the potential uses or value of CTY.

7) Risk that the Contingency Network, As Developed, Will Not Meet the Expectations of Purchaser

The Contingency network is presently under development and may undergo significant changes before release. Any expectations regarding the form and functionality of CTY or the Contingency network held by the purchaser may not be met upon release, for any number of reasons including a change in the design and implementation plans and execution of the Contingency network.

8) Risk of Theft and Hacking

Hackers or other groups or organizations may attempt to interfere with the Contingency network or the availability of CTY in any number of ways, including without limitation denial of service attacks, Sybil attacks, spoofing, smurfing, malware attacks, or consensus-based attacks.

9) Risk of Security Weaknesses in the CTY network Core Infrastructure Software

The Contingency network constsists of opensource software that is itself based on open-

source software. There is a risk that the Contingency team, or other third parties may intentionally or unintentionally introduce weaknesses or bugs into the core infrastructural elements of the Contingency network interfering with the use of or causing the loss of CTY.

10) Risk of Weaknesses or Exploitable Breakthroughs in the Field of Cryptography

Advances in cryptography, or technical advances such as the development of quantum computers, could present risks to cryptocurrencies and the Contingency platform, which could result in the theft or loss of CTY.

11) Risk of CTY Mining Attacks

As with other decentralized cryptographic tokens and cryptocurrencies, the blockchain used for the Contingency network is susceptible to mining attacks, including but not limited to doublespend attacks, majority-mining power attacks, 'selfish-mining' attacks, and race condition attacks. Any successful attacks present a risk to the Contingency network, expected proper execution and sequencing of Contingency markets, and expected proper execution and sequencing of Ethereum contract computations. Despite the efforts of the Contingency Team, the risk of known or novel mining attacks exists.

12) Risk of Lack of Adoption or Use of the Contingency Network

While CTY should not be viewed as an investment, it may have value over time. That value may be limited if the Contingency network lacks use and adoption. If this becomes the case, there may be few or no markets upon the launch of the platform, limiting the value of CTY.

13) Risk of an Illiquid Market for CTY

There are currently no exchanges on which CTY might trade. If exchanges do develop, they will likely be relatively new and subject to poorly understood regulatory oversight. They may therefore be more exposed to fraud and failure than established, regulated exchanges for other products. To the extent that the exchanges representing a substantial portion of the volume in CTY trading are involved in fraud or experience security failures or other operational issues, such exchanges' failures may result in a reduction in the value or liquidity of CTY.

14) Risk of Uninsured Losses

Unlike bank accounts or accounts at some other financial institutions, funds held using the Contingency or Ethereum network are generally uninsured. In the event of loss or loss of value, there is no public insurer or private insurer to offer recourse to the purchaser.

15) Risk of Dissolution of the Contingency Project

It is possible that, due to any number of reasons, including without limitation an unfavorable fluctuation in the value of Bitcoin, unfavorable fluctuation in the value of CTY, the failure of business relationships, or competing intellectual property claims, the Contingency project may no longer be a viable business and may dissolve or fail to launch.

16) Risk of Malfunction in the Contingency Network

It is possible that the Contingency network malfunctions in an unfavorable way, including but not limited to one that results in the loss of CTY, or information concerning a market.

17) Unanticipated Risks

Cryptocurrency and cryptographic tokens are a new and untested technology. In addition to the risks set forth here, there are risks that the Contingency team cannot anticipate. Risks may further materialize as unanticipated combinations or variations of the risks set forth here.