FunFair 기술 로드맵 및 토론

2017년 6월 6일, v0.97

제레미 롱리(Jeremy Longley)와 올리버 홉튼(Oliver Hopton)

내용

1. 소개

FunFair의 기술 플랫폼은 전 세계 어디에서나 즐길 수 있는 차세대 게임을 제공하기 위해 설계된 야심찬 프로젝트입니다. 이 문서는 FunFair의 설계 목표, 구현 및 향후 로드맵에 대해 설명합니다.

FunFair 플랫폼에 대한 전체 개요는 https://funfair.io/의 백서를 참조하시기 바랍니다.

2 면책 조항 및 공지

여기에서 논의 된 기술 개발의 일부는 미국, 유럽 연합, 아시아 및 전세계의 다른 시장에서 출원중인 특허에 의해 보호 될 수 있습니다. 미래 지향적인 모든 정보는 본질적으로 투기적이며 기술, 규제 및 시장 움직임을 비롯한 수 많은 외부 변수에 따라 변경 될 수 있습니다.

3 디자인 목표

저희의 핵심 목표는 차세대 대응 온라인 게임 환경을 위한 플랫폼과 프로토콜을 구축하는 것입니다.

플랫폼의 모든 게임은 다음과 같은 엄격한 기준을 충족해야합니다.

입증된 공정성(Provably Fair) 블록체인을 통해 게임 플레이를 확인해야합니다.

은행이 없는(bankless) 블록체인을 통한해 거래를 저장해야합니다.

즉각적인(Fast) 사용자가 UI 버튼을 누른 후, 결과를 보기까지의 대기 시간이 없어야합니다.

유연한(flexible) 게임 세션 중 다음과 같은 플레이어들의 선택을 허용해야합니다.

• 게임에서 게임으로 베팅의 크기를 다양화 가능
• 상금으로 즉시 플레이 가능
• 중간에 자금 추가 가능

4 난수 생성

카지노 게임의 핵심은 난수 생성기(RNG)입니다. 모든 소프트웨어 기반 RNG는 사실상 의사 난수 생성기 (PRNG)입니다.

블록 체인에 대한 PRNG는 많은 문제점을 가지고 있습니다.

거래 하나 당 일부 블록 체인 게임은 한 번에 하나의 무작위 게임을 생성합니다. 느리고 값 비싼 방식으로 플레이어나 운영자에게는 적합하지 않은 방법입니다. 또한, 일반적으로 비밀 정보에 대해 매일의 "결정과 공개(commit and reveal) "가 요구됩니다. 게이머는 운영자가 속임수를 쓰지 않았음을 확인하고, 반드시 게임 도중 신뢰해야합니다. 사토시 주사위 (Satoshi

Dice)와 같은 설정값을 사용하는 구식 게임은 내기가 걸리기 전에 최대 1-5 달러의 비용이 들 수 있으며, 블록이 남은 정도의 시간에 따라 내기 당 몇 분에서 몇 시간이 걸릴 수 있습니다.

오라클(Oracles) 다른 블록 체인 기반의 온라인 게임은 임의성(randomness)을 유발하기 위해 **오라클 (Oracles)**을 사용합니다. 이 경우 속도가 느리고, 블록체인 확인 속도에 의해 제한되고, 결과를 얻기 전에 여러 블록을 채굴해야 하는 경우가 종종 있으며, 운영자, 직원 및 서버에 대한 어려운 인센티브 질문을 추가해야합니다.

블록 해시(Block Hashes) 난수 생성을 위한 최악의 사용 블록 해시입니다. 일단 느리고, 근본적으로 채굴자들의 공격에 취약합니다.

이 기술들 중 어느 것도 2017년, 고사양의 게임을 만드는 데 사용할 수 없습니다.

5 독자적인 솔루션 : 페이트 채널(fate channel)

저희는 플레이어와 운영자에 의해 개별적으로 제공된 일부 RNG 시드(seeds)를 포함하는 상태 채널(state channel)을 사용하여 입증된 공정성(Provably Fair)의 시스템을 개발했습니다. 이 부분적인 시드(seeds)는 게임 세션이 시작될 때 블록 체인에 설치됩니다.

상태 채널(state channel)은 참가자가 예탁한 금액으로 갱신 된 "클레임"에 대해 신속하게 다른 사람이 서명한 문서를 인정하는 '서명인 첨서(countersigning)'를 할 수 있게 작동합니다. 비트코인 라이트닝(Bitcoin Lightning) 프로토콜은 이 아이디어를 대중화하기 위한 첫 번째 시도였습니다. 이더리움VM을 사용할 수 있는 블록체인에서는 상태 채널(state channel)이 매우 간단하고, 그 구현이 쉽습니다. 스마트 계약서는 예탁된 자금을 저장하고, 상태 채널(state channel)의 참가자가 요청할 때 자금을 풀어줍니다.

게임을 하는 동안 저희는 대신 "페이트 채널(fate channel)"을 만듭니다;

결정론적인, "운명(fate)"이지만, 페이트 채널(fate channel)에서는 예측할 수 없는 난수 연속성을 발전시켜, 양 당사자 간의 점직전인 공개기법(reveal scheme)을 검증 할 수 있게 되었습니다.

페이트 채널(fate channel) 구현의 세부 사항은 저희의 토큰 판매를 따를 것입니다. 현재로서는 세부 구현 정보를 조금 더 오래 비공개로 유지하는 것이 토큰 소유자와 저희에게 유리한 경쟁 위치를 제공한다고 생각합니다.

6 개발 연혁

저희는 초기 비교적 복잡한 슬롯 게임인, 30 개의 윈-라인 (30 win-lines), 와일드 카드(wild cards), 스캐터 심볼(scatter symbols) 등 무료 스핀(free spins)을 특징으로하는 보너스 모드로 시작했습니다.

온라인상의 많은 슬롯 게임은 결과를 먼저 결정한 다음 릴(reels)의 위치를 결정합니다. 이후 릴(reels)을 적절한 위치로 이동시킵니다. 하지만 이 방법은 향후 게임의 복잡성을 제한할 뿐만 아니라 실제 슬롯 머신이 작동하는 방식이 아니기 때문에 슬롯 그래픽이 겹쳐지는 게임인 주사위 게임(dice game)과 비슷하게 '가짜 슬롯(fake slot)'으로 간주 될 가능성이 있습니다.

'숫자를 선택하고 움직이십시오(pick a number then animate)'라는 솔루션은 기술적으로 막다른 길 (dead end)입니다. 블랙 잭(Blackjack)과 룰렛(Roulette)과 같은 복잡한 게임은 이 방법으로 쉽게 변환되지 않으므로, 저희는 준비 과정에서 '어려운 방법(hard way)'을 선택해 구현했습니다.

6.1 FunFair 슬롯 v0.1

블록체인에서 슬롯 머신의 규칙을 인코딩했습니다. 처음에는 스마트 계약서에서 향후 블록을 선택하고, 난수 생성기 (RNG)의 시드(seeds)를 사용하는 시스템을 구축했습니다. 적절한 양의 블록이 채굴되면, 계약서는 이전에 채굴 된 블록의 해시를 사용하고, 불확실성, 즉 엔트로피(entropy)를 생성하기 위해 적절하게 조치를 취한(salted)다음, 스마트 계약으로 암호화 된 상태머신(state machine)을 통과합니다. 이 상태머신(state machine)은 슬롯 머신의 각 릴(reels)의 위치를 결정합니다.

이것은 난수를 얻는 잘못된 방법입니다. 채굴자들은 내재적 요인의 수에 따라 손실이 있는 경우 채굴 된 블록을 버릴 수있는 인센티브를 가질 수 있기 때문에 이 방법으로 채굴자가 게임을 하는 경우 운영자에게 위험을 초래합니다.

6.2 슬롯 v0.1 향상

저희는 다음 두 가지 방식으로 기본 게임을 확장했습니다.

멀티 스핀(Multi-Spin) 플레이어는 하나 이상의 스핀에 대해 자금을 "삽입"할 수 있습니다 - 생성 된 엔트로피(entropy)는 한 번에 하나씩이 아닌 일련의 스핀을 결정하는 데 사용될 수 있습니다. 즉각적인 속도의 게임을 제공하는 첫 번째 혁신의 핵심입니다.

무료 스핀(Free Spins) 초기 시드(seeds)를 통해 여러 개의 스핀을 만들 수 있으며, 스핀을 추가하기 위해 시스템 기능을 확장했습니다. 여전히 동일한 난수로 시드되었습니다.(seeded).

이 시스템은 저희 의도대로 개발되고 작동할 것입니다. 상징적인 애니메이션과 효과를 포함하여 구축한 세련된 웹 기반의 프론트 엔드(front end)를 통해, 저희의 기술력을 확인하실 수 있을 겁니다.

사진과 동영상 링크는 https://funfair.io/whitepaper에서 확인하시기 바랍니다.

6.3 v0.1의 문제점

초기 프로젝트의 성공을 통해, 블록체인에서 재미있고,즉각적인 속도의 고사양 슬롯 머신을 구축 할 수 있다는 것을 입증했습니다.

이 시스템은 저희의 핵심 요구 사항을 충족하지 못했습니다. 채굴자가 악용 할 수 있었고, 게임 중간 결정(mid-game decisions)을 허용하지 않았으며, 가스 비용이 금지되었습니다.

여기서 채굴자의 부정 행위를 사전에 방지하는 몇 가지 개선안을 제안했지만, (결정과 공개 계획(commit/reveal scheme)으로 채굴 순간에 RNG에 대한 정보를 가리는 것) 더 나은 방법을 찾기로 했습니다.

6.4 v0.2의 설계 목표

v0.1의 PRNG 계획은 재미있고, 빠르며, 공정하고 유연한 게임을 만들고 싶은 저희의 목표와 부합하지 않았습니다. 다른 해결책을 찾았고, 우리는 블록 체인 및 게임 커뮤니티의 3 가지 연구 영역을 통합했습니다.

상태 채널(fate channel) 상태 채널을 통해, 오프 체인(off-chain) 상태에서 당사자 간 직접 극소량의 이체(micro-transactions)를 처리 할 수 있습니다. 자금은 사전에 스마트 계약으로 체결, 고정됩니다. 거래는 당사자 간에 발생하며 계속적으로 모든 사람이 서명합니다. 국가는 모든 당사자가 결과에 동의 함을 입증하는 방식으로 체인에 다시 투입됩니다. 최종 상태(final state)는 모든 당사자가 결과에 동의 함을 입증하는 방식으로 체인에 다시 투입됩니다.

입증된 공정성(Provably Fair) 기본 개념은 일부 엔트로피(entropy)가 사전에 블록 체인에 암호화되어 투입되었다는 것입니다. 게임 플레이가 발생하면이 엔트로피(entropy)가 게임에 사용되는 RNG 소스였음을 알 수 있습니다. 스마트 계약에서 게임 규칙을 인코딩하는 것과 함께 게임의 공정성을 증명할 수 있습니다.

역방향 해시 체인(Reverse Hash Chains) 해시 체인을 만들려면 안전한 초기 시드(seed)를 선택하고, 해시하고, 해시를 다시 해시하고, 이를 여러 번 반복 하며 마지막 해시를 표시합니다. 공개 할 때 ,일련의 비밀 난수가 만들어지며, 그 순서는 한 번에 하나씩 역방향으로 나타날 수 있습니다. 공개자는 해시 알고리즘을 깨지 않고 속임수를 쓰거나 마음을 바꿀 수 없습니다. 이전 번호를 순서대로 표시해야 하며, 이 번호는 올바른 '이전' 비밀 번호로 쉽게 확인할 수 있습니다.

6.5 페이트 채널(fate channel) v0.2

FunFair의 슬롯 머신 뒤에서 궁극적으로 난수 생성을 강화하기 위해 저희는 오프 블록 체인(off- blockchain)으로 작동하는 난수 생성기를 개발했습니다. 이것은 게임 세션 기간 동안 상태 채널(state channel)로 존재하며, FunFair 클라이언트와 서버 간의 실시간 대화(messaging)를 지원합니다.

저희는 이 채널을 "페이트 채널(fate channel)"이라고 부릅니다.

6.5.1 채널 설정

페이트 채널 (Fate Channel)은 플레이어(클라이언트)와 카지노(운영자)간의 게임 세션 전반에 걸친 통신을 지원합니다. 저렴하고 신속한 방법으로 난수 생성, 게임 세션 시작, 종료, 블록 체인에서의 스마트 계약 체결 등을 제공합니다.

각 게임에 대해 스마트 계약 API 호출이 게임의 규칙을 압축하여 발행됩니다. 가장 중요한 페이트 채널 (fate channel) 계약은 기본적으로 두 가지를 이행 합니다. 게임 세션을 시작하고,하나를 정착(settle) 시킵니다 (또는 종료합니다).

6.5.2 클라이언트(client)

클라이언트는 블록 체인 및 서버와 통신 할 수있는 웹 기반, 자바 스크립트 및 HTML5 / WebGL 응용 프로그램입니다. 미래에는 클라이언트가 모바일의 기본 응용 프로그램이 될 수 있지만, 현재는 모바일 브라우저에서 직접 작동되어, 최대한 많은 고객이 액세스 할 수 있도록 돕습니다.

6.5.3 서버

서버는 클라이언트와 매우 유사하지만 사용자 상호 작용이 없습니다.

플레이어가 게임 세션을 시작하면 클라이언트와 서버 모두 역방향 해시 체인(reverse hash chains)을 만듭니다. 페이트 채널(fate channel) 계약은 양 플레이어의 모든 상호 작용을 검증하고, 블록 체인에 세션을 생성하고, 자금을 잠그고, 블록체인에 이벤트를 게시합니다.

6.5.4 프로토콜

게임이 진행됨에 따라 클라이언트와 서버는 보낸 사람이 서명 한 거래 메시지를 교환합니다.

세션의 상태가 주어진 메시지에서 진행되면 새로운 상태가 서명 되고, 이전 상태 (이미 상대방이 서명 한)에 공동 서명됩니다. 게임 세션의 각 결과에 대해 서버는 역방향 해시 체인(Reverse Hash Chain)에서 다음 해시를 가져와서 다음 클라이언트 해시(클라이언트가 제공함)와 결합하여 해시를 취하여 RNG를 만듭니다.

그런 다음 이 RNG를 사용하여 게임 로직(logic)을 실행하고,게임 상태 머신(state machine)에서 액션을 결정합니다. 한편, 클라이언트는 서버와 같은 방법으로 동일한 해시를 사용하여 RNG를 생성합니다. 게임 로직(logic)의 자체 구현을 통해 우승 및 기타 게임 결과가 서버의 결과와 일치하는지 검증합니다.

세션을 끝내려면 플레이어는 현금 지급 버튼을 누릅니다. 클라이언트는 가장 최근 거래 상태에 서명하고, 서버는 공동 서명과 함께 "세션 종료"메시지로 페이트 채널(fate channel) 계약을 완료합니다. 계약은 모든 관련 데이터를 광범위하게 검증합니다. 모두 완벽한 상태라면, 계약서는 남은 자금을 지불하고, 세션은 끝이 납니다.

6.5.5 온체인(On-Chain) 검증

이 초기 구현은 안전하고, 결정론적이고(deterministic), 공정한 게임 플레이를 가능케합니다. 그러나, 저희는 이것을 온체인에서 검증하고자 합니다. 이렇게 하려면 두 가지 추가 계약 방법이 필요합니다.

체인 검증(Chain Verification) 클라이언트와 서버에 의해 생성 된 역방향 해시 체인(Reverse Hash Chains)을 각각 확인하기 위해 사용 된 마지막 해시가 체인에 게시됩니다. 페이트

채널(Fate Channel)은 이것을 정확한 횟수만큼 해시하고, 체인에 맡겨진(committed) '최종 해시(final hash)'를 다시 만들 수 있습니다.

게임 검증(Game Verification) 개별 게임을 검증하기 위해 게임 상태 머신(state machine)을 게임 유형별로 하나씩별도 계약으로 블록체인에 구현합니다. 이 함수는 상수 함수가 될 수 있습니다. 초기 시드(seeds)와 게임 간의 출력을 가져 와서 참(true) 또는 거짓(false)을 반환합니다. 상수 함수는 블록 체인을 수정하지 않으므로, 모든 참가자는 이를 무료로 호출하고 실행할 수 있습니다..

7 운명 채널 v2

다음 개발 단계에서는 두 가지 개선점이 있습니다.

임시 채널(Ephemeral Channel) 페이트 채널 (fate channel) v1에서 클라이언트는 채널 메시지에 서명하기 위해 임시(Ephemeral)키를 생성합니다. 고객이 너무 오래 기다리다 주소 서명 키를 잊어버릴 수도, 웹 3 클라이언트에서 거래 청구를 위한 이체를 다시하지 않으려 할 수도 있습니다. 클라이언트는 인터페이스 요청이 마찰을 불러 일으키거나 산만해지면 그냥 브라우저 창을 닫고 떠날 수 있습니다. 클라이언트 서명 키는 세션과 함께 페이트 채널(fate channel) 계약에 암호화되어 저장 될 수 있습니다. 저희는 이것으로 부분 세션도 복구 할 수 있다고 생각합니다.

통합 상태 머신(Unified State Machine) 페이트 채널 v1(Fate Channels v1)은 스마트 계약, 클라이언트와 서버의 세 가지 위치에 로직(logic)을 저장합니다. 때때로 이들은 서로 다른 언어 (Solidity, Javascript 및 (현재) C #)로 구현됩니다. 저희는 이들을 통합하는 방법을 모색하고 있습니다. 표준화 된 상태 머신 구조(standardized state machine) 또는 클라이언트와 서버가 이더리움 블록체인의 상수 기능만 사용하도록 하는 등의 방법도 있습니다.

8 페이트 채널(Fate Channels) v3 : 다중 상태 게임(Multi-State Games)

FunFair 슬롯 머신은 페이트 채널(fate channel)이 이체 비용을 높이거나 블록 체인을 스팸하지 않으면서, 더 빠르고, 공정한 게임을 제공 할 수 있다는 것을 증명합니다. 이를 가능케 하는 저희는 전 세계 유일무이한 기술력을 갖춘 게임 회사이고, 앞으로도 더 발전할 것입니다. 슬롯 머신, 주사위 게임 및 룰렛은 "지르고 잊자(fire and forget)"라는 방식으로, 일단 플레이어가 바퀴를 돌리거나 주사위를 던지면 내기를 바꾸거나 결과에 영향을 줄 수 있는 중간 플레이(mid-play)를 할 수 있는 방법이 없습니다.

"다중 상태(multi-state)"게임은 전 세계적으로 인기가 더 많습니다. 플레이어가 자신의 베팅(블랙잭)을 변경하거나, 이전 베팅 (크랩스)의 결과에 새로운 베팅을 할 수 있는 등 어떤 방식으로든 게임에 직접 영향을 미칠 수 있기 때문입니다.

블랙잭(Blackjack)과 같은 여러 상태(multi-state) 게임을 지원하기 위해 FunFair는 페이트 채널(Fate Channel)의 프로토콜을 강화할 것입니다. 이러한 변경을 통합하는 페이트 채널(Fate Channel) v3는 2017년 3분기에 발표 할 예정입니다.

9 페이트 채널(fate channel) v4 : 완전한 사용자간 직접 접속 (P to P, peer-to-peer)

페이트 채널(Fate Channel)은 서버와 클라이언트를 생각합니다. FunFair는 두 번의 클릭만으로 운영자가 직접 서버를 실행할 수 있도록 만들 계획입니다. 롱테일(long tail) 운영자, 개인 그룹, 유명 인사 및 기타 모든 사람들이 손쉽게 양질의 게임을 운영하게 하는 것, 누구나 자신만의 게임 환경을 시작하고 운영 할 수 있도록 하는 것이 바로 저희가 추구하는 핵심 가치입니다.

페이트 채널(Fate Channel) 항목에서 서버 구성 요소를 완전히 제거할 예정이며, 이를 수행 할 수 있는 방법이 있다고 생각합니다. 성공한다면 블록 체인의 분산되고, 분권화 된 성격을 십분 응용할 수 있습니다.

이것은 기술적으로 95 %의 성공 확률을 가진 도전적인 혁신입니다. 초기 결과가 좋았으며, 모든 FunFair 이해 관계자들에게 큰 이익이 될 수 있기 때문에 저희는 성공을 위해 최선을 다해 추진할 예정합니다.

저희는 현재 서버가 전혀 없는(serverless), 누구나 재미있고, 빠르고, 공정한 게임을 할 수 있는, 모든 핵심 사항을 충족시키는, 완벽한 P2P 게임을 2017년 4분기에 발표하기 위해 노력 중입니다.

10 암호 체계에 대한 주의 사항

암호체계 - 예를 들어 String Labs의 Dynity 프로젝트로 대중화 된 BLS는 블록 당, 최소 하나의 참가자 그룹에 의해 생성 된 정말 안전한 난수를 보장하지만, 이러한 암호법 기본 요소는 이더리움의 메트로폴리스 제품(zk-Snarks에 대한 지원도 추가하는)과 기타 개인정보 보호정책에서도 지원됩니다.

이 기술을 통합하기 위해 메커니즘(mechanisms)을 업데이트 할 수도 있지만, 게임의 "즉각적인 반응 속도(instant)”를 위해서 계속해서 페이트 채널(fate channel)을 사용할 것입니다. 채널 생성의 시작과 끝보다, RNGs를 더 자주 사용함으로 가스 비용(gas costs)이 많이들 것입니다.

저희는 이더리움 인프라의 개발 속도를 감사하게 여기며, 더 나은 서비스 제공을 위해 새로운 기능과 연구를 지속적으로 평가하고 있습니다.

11 추가 정보

더 자세한 기술 정보는 웹 사이트 https://funfair.io를 확인하거나, info@funfair.io로 주소로 메일을 보내주시기 바랍니다.