

암호화폐의 미래: 분산금융채널

Hyoung Joong Kim
Korea University

khj-@korea.ac.kr 010-6251-6343

해시넷

2019. 10. 15.

미디어



코인위키

코인뉴스

코인칼럼

코인동영상

채굴

코인위키

대문

- 블록체인
- 암호화폐
- 거래
- 채굴
- 인물
- 기업

둘러보기

- 대문
- 최근 바뀐
- 임의 문서로
- 도움말

문서 토론

읽기 편집 역사 보기 검색

㈜해시넷이 2019년 3월 7일(목) 18:30에 제1회 ㈜해시넷 블록체인 밋업을 진행합니다.

비트베리

비트베리(BitBerry)는 **두나무**(주)의 자회사로 편입된 **루트원**(Root One)에서 개발한 **암호화폐 지갑**이다. 보통 다른 암호화폐 지갑들은 송금하고자 하는 코인으로 생성된 **토큰**일 경우, 해당 디앱의 주소를 등록하고 송금 대상자의 지갑 주소로 송금하는 절차를 거치게 되지만, 비트베리 지갑은 SNS 계정으로 로그인하기 때문에, 단순히 상대방 전화번호만 알면 송금할 수 있다. 2018년 기준으로 비트베리 지갑은 카카오톡 계정만 지원하고 있다. 플랫폼 코인은 비트코인만 사용 가능하다. 안드로이드와 iOS용 모바일 앱을 설치해서 사용할 수 있으며, PC용 웹 버전은 향후 추가할 계획이다.

목차 [숨기기]

- 1 특징
- 2 모스랜드 게임
- 3 향후 계획
- 4 같이 보기

coindesk

6,173

Medium

182

StackExchange

112

Quora

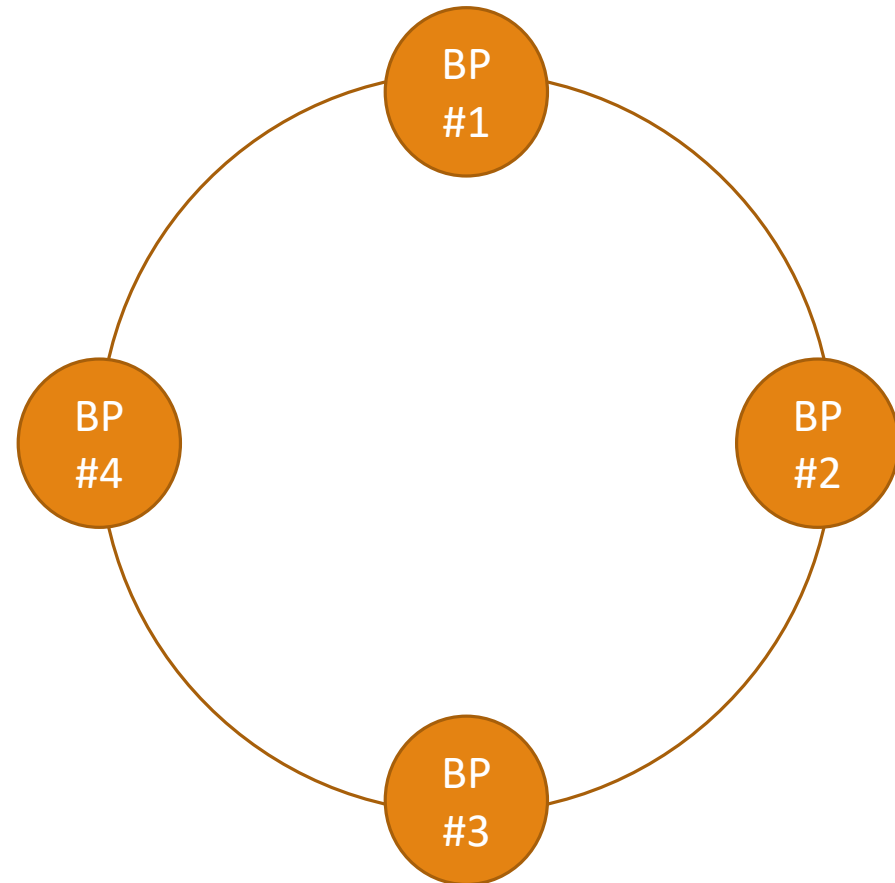
81

stackoverflow

49

Alexa rank at 2019-09-15

Cheating in Betting



Fair random number generator?

Verifiable Delay Function



Time-Lock Puzzle

$W_{k+1} = W_k^2 \bmod n$
(병렬계산 불가, 역함수 부재)

$$\begin{aligned}W_{67} &= 8711^2 \bmod 9797 = 3756 \\W_{68} &= 3756^2 \bmod 9797 = 9653 \\W_{69} &= 9653^2 \bmod 9797 = 1142 \\W_{70} &= 1142^2 \bmod 9797 = 1163 \\W_{61} &= 1163^2 \bmod 9797 = 583 \\W_{67} &= 583^2 \bmod 9797 = 6791\end{aligned}$$

Verifiable Delay Function

병렬계산 불가, 난이도 t 일 때 $\log(t)$ 내 확인 가능

Ethereum RANDAO

결론

암호화폐 산업이 지향해야 할 지점

분산금융산업

- 분산금융산업에 필요한 기능 구현 가능한 기술 개발 필요
- 분산금융채널에 적합한 비즈니스 모델 발굴 필요