UNIVERSITY of NICOSIA

Session 11

Dapps – Decentralized Prediction Markets

BLOC 514: Emerging Topics in Blockchain and Digital Currency

Session Objectives

- To introduce prediction markets and explain their relation to cryptocurrencies and blockchains
- To explain how the concept and "wisdom of crowds" applies to the case of prediction markets
- To present the key idea of decentralized exchange markets and discuss the pros and cons of centralized vs. decentralized
- To provide an overview of indicative platforms that operate in the context of predictions markets and decentralized exchange markets

The fundamental properties of blockchains enable the development of prediction markets within a decentralized context. In this session, we will discuss this potential along with a series a challenges that remain open. Also, we will present the pros and cons of decentralized exchange markets.

Agenda Slide

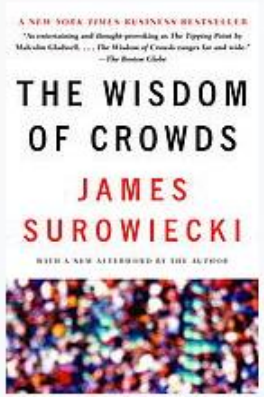
- Prediction markets
- Oracles
- Prediction markets: platforms
- Decentralized exchanges
- Decentralized exchanges: platforms
- Conclusions
- Resources

Prediction markets: Introduction

- Prediction markets are based on binary events
  - A binary event is characterized by two values:
    - Will happen (“1”)
    - Will not happen (“0”)
- Prediction markets enable the trading of future events
  - Examples: elections, company sales, price of commodities, etc.
  - Can be regarded as the assignment of bets on the likelihood of futures events
- Under certain conditions (*), the value of a bet for a given event approximates the probability of occurrence of this event
  - (*) Large number of individual predictions – wisdom of crowds

Prediction markets: Introduction

The Wisdom of Crowds



Cover of mass market edition by Anchor

Author	James Surowiecki
Country	United States
Language	English
Publisher	Doubleday; Anchor
Publication date	2004
Pages	336
ISBN	978-0-385-50386-0
OCLC	61254310
Dewey Decimal	303.3/8 22
LC Class	JC328.2 .S87 2005

Source: https://en.wikipedia.org/wiki/The_Wisdom_of_Crowds

Prediction markets vs. gambling

- Gambling is mostly determined by luck (randomness)
  - Randomness: lack of predictability, i.e., lack of regularities (patterns) in related data
  - Example of random (binary) event: coin flip – 50% head, 50% tails
  - Absence of external factors that affect the event under prediction
    - Strictly speaking: at least, not known factors
  - As a result, no effort is devoted for developing prediction models
- Prediction markets are quire different compared to gambling
  - Payoffs depend on the accuracy of predictions
    - So, effort is put to develop accurate models
    - Example: market research
  - Prediction markets depend of collective wisdom
    - "Collective wisdom": research conducted by a group of people

Operation of prediction markets: Futures

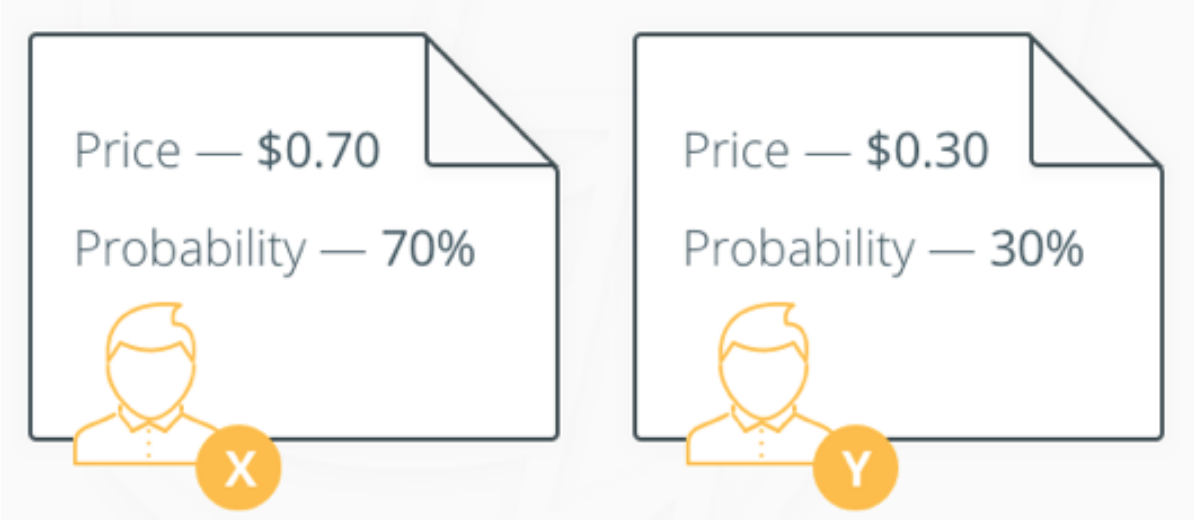
- Futures: an agreement regarding buy & sell action with respect to an asset
  - Specific future date
  - Specific date
- The involved parties buy & sell according to the pre- determined price regardless of the market price at the specified date
  - The aim of such agreements is not the maximization of the profit
  - Futures used as a risk management tool: all parties are protected against price volatility
- Example
  - Assume a seller that trades an asset at $3 per unit. A buyer (who expects the price of this asset to increase in the near future) buys a 5-month futures contract for 1000 units at the current price. The value of this contract equals $3000.Hypothesize that after 5 months the price of this asset is $3.5 per unit. Through the futures contract the buyer has saved $500.
- The speculation of futures contracts also takes place rather than the utilization of them as a protection mechanism

Operation of prediction markets: Cryptocurrency futures

- The contract relies on the price of the cryptocurrency of interest
  - Specifically, the speculators place bets according to their estimations about the future price of the cryptocurrency
  - Interestingly, one can place such bets without the requirement of owning cryptocurrencies
- Two basic consequences
  - The cryptocurrencies can remain unregulated, while the respective futures can exist in regulated environment. This can be regarded as a positive feature for those who are concerned about the lack of regulatory framework.
  - In countries where the trading of cryptocurrencies are not permitted, the speculators may have to opportunity to speculate on cryptocurrency-based futures.
- Can futures make the price of (major) cryptocurrencies less volatile?
  - In principle, yes (in combination with a series of other conditions, e.g., adoption by institutional investors)

Operation of prediction markets

- Example: presidential elections
- Candidate X: Assume that X's contract trades at $0.70
- Candidate Y: Assume that Y's contract trades at $0.30
- If your speculation proved to be correct then you get $1.00, otherwise you get $0.00



Source: https://cointelegraph.com/explained/prediction-markets-explained

Operation of prediction markets: Wisdom of crowds

- Collective view vs. individual predictions
  - A group of people is expected to have more information compared to individuals
  - As a result, the predictions based on collective view tend to be more accurate than the individual predictions
- What distinguishes the wise crowd from the irrational mass
  - Diversity of views
  - Independence of views
  - Decentralization of views
  - Aggregation of views
- The role of economic incentive
  - The effort is proportional to the economic incentive

Operation of prediction markets: Oracles

- Definitions
  - Oracles in mythology: provided information exploited for decision making in cases of uncertainty (lack of knowledge)
  - Similar situation in blockchains: no access to the out-of-the-chain world
- Main characteristic of off-chain world
  - Non-deterministic: continuous changes, low predictability
  - Opposed to the deterministic character of blockchains: certainty about the status of transactions
    - Data immutability, but low flexibility
- Importance for smart contracts
  - Verification of the conditions (terms) upon which smart contracts are developed
  - Examples of such terms: status of payments, prices, etc.
- Overall: oracles connect blockchains with the outside world

Prediction markets: Decentralization

- Decentralization of trades and bets
  - Elimination of central authorities
  - Significant reduction of fees
- Transparency of information
  - Centralized prediction markets: the central authority can withhold information related to predictions in order to favor a selected subset of market participants
  - Decentralized prediction markets: information is publicly available
- Challenge
  - Not all events are well-known
  - Need to dispute resolution
  - Example: Kleros – A blockchain dispute resolution layer

Prediction markets: Augur

- Founded in 2014
  - By Jack Peterson and Joey Krug
  - Legal entity: Forecast Foundation (not-for-profit corporation)
  - Board of advisors include Vitalik Buterin
  - Based on Ethereum's blockchain
  - Native reputation token: REP
- July 2020: version 2
  - Numerous changes (including the use of DAI)
- White paper (version 2 – Aug 2022 update): pdf

Prediction markets: Gnosis

- Founded in early 2015
  - Board of advisors include Vitalik Buterin
  - Native token: GNO
  - Based on Ethereum's blockchain
  - Targets: financial, insurance and information markets
  - Long-term goal: collection of data generated by AI-based systems in order to enable accurate forecasts
- Trading of predictions
  - Done in ETH
- Event creators
  - Pays only Ethereum gas costs
- Research paper: pdf

Decentralized exchanges

Why? Just see the following recent incident

Nov 2022

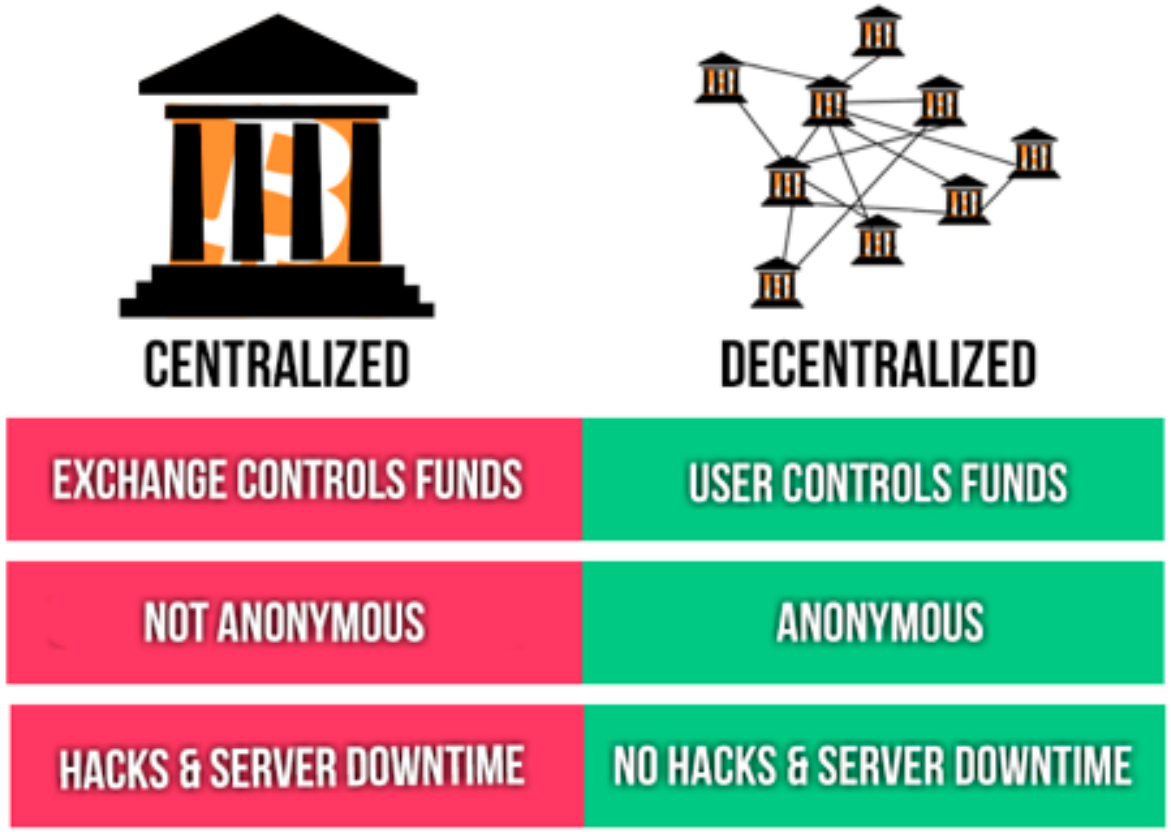
Decentralized exchanges

- Decentralized exchange: an exchange market that does not utilize third party services
  - Trades take place between users (pert-to-peer) automatically
- Current situation: the majority of cryptocurrency exchanges rely on centralized components
  - IOU ("I owe you") trading model
  - In practice, a representation of currencies is used during trading
  - The currencies are redeemed in real currencies when the user withdraws them
  - User gains control only when the trading actions have been processed and the currencies have been withdrawn
  - Overall, the IOU model assumes high level of trust
- Importance of decentralized exchanges for cryptocurrencies
  - First of all: alignment with the ideology of decentralization
  - Also: security (centralized systems: weak points for attacks)

Decentralized exchanges

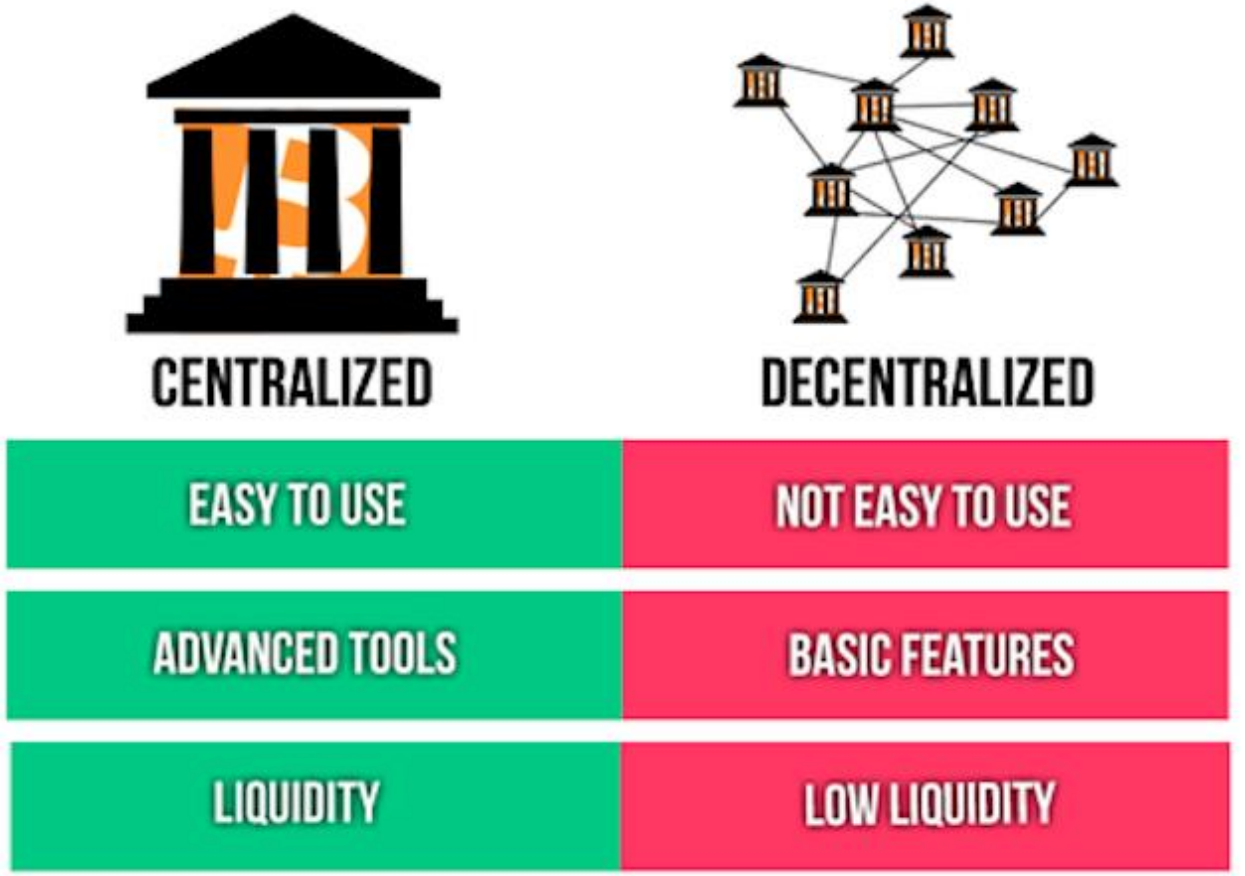
- Given an exchange, check the following:
  - Requirement of email or other similar account (e.g., Facebook) for signing up
  - Coins transferred to a third party address
  - Use of intermediate token(s)
  - The exchange is run by a central entity
  - Part of profits go to a third party entity
  - Existence of withdrawal limits
  - The order books and order matching are centralized
  - Any core function is centralized
  - Existence of exchange costs
  - Specific pairs of coins can be traded
- If any of the above holds, then the exchange is **not truly decentralized**

Decentralized exchanges: Benefits



Source: https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/

Decentralized exchanges: Downsides



Source: https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/

Top decentralized exchanges (by 24h trading volume)

#	Exchange	24h Volume	Num Coins	Num Pairs	Visits	Most Traded Pair	% Market Share By Volume
1	Uniswap (v3) Decentralized	$762,574,254	852	1533	3,028,974.0	USDC/0XC02... $375,170,420	46.4%
2	Curve (Ethereum) Decentralized	$175,114,038	45	85	439,693.0	USDC/0XDAC... $84,213,441	10.7%
3	PancakeSwap (v2) Decentralized	$87,615,144	3311	3720	6,077,049.0	WBNB/USDT $15,451,607	5.3%
4	DODO Decentralized	$66,313,273	9	22	101,699.0	USDT/USDC $43,995,905	4.0%
5	Balancer (v2) Decentralized	$62,675,687	72	96	113,142.0	BB-A-USDT/... $22,644,925	3.8%
6	Uniswap (v2) Decentralized	$52,055,171	1389	2413	3,028,974.0	WOOL/0XC02... $13,596,205	3.2%
7	Uniswap (Polygon) Decentralized	$44,968,430	153	459	3,028,974.0	USDC/0X7CE... $13,754,829	2.7%
8	Uniswap (Arbitrum One) Decentralized	$40,497,202	69	187	3,028,974.0	WETH/0XFF9... $30,162,069	2.5%
9	Apex Pro Decentralized	$39,546,737	6	7	0	BTC/USDC $30,371,103	2.4%
10	Uniswap (Optimism) Decentralized	$17,716,622	37	143	3,028,974.0	WETH/0X7F5... $8,158,846	1.1%

Source: https://www.coingecko.com/en/exchanges/decentralized

Conclusions

Conclusions

- Prediction markets
  - Application of an existing idea in the context of cryptocurrencies and blockhains due to the related properties
    - Decentralization, transparency of information, smart contracts, collective intelligence, etc.
  - Different with respect to gambling
  - Main challenges: verification of events, dispute resolution
- Decentralized exchange markets
  - Currently, the majority of platforms are (at some extent) centralized
  - As a result, the user has no full control during the entire trading process
  - Main challenge: development of 100% decentralized platform that exhibits the desirable features of a centralized system
- Both areas (prediction markets and decentralized exchange markets) constitute a very active field of research and development.

Bibliography

References

- A. Lehar and C. A. Parlour, "Decentralized Exchanges"
  - Only Section 1 (excl. sub-section 1.1)
- "Understanding a Decentralized Exchange"

Additional Bibliography (optional)

- Todd Proebsting. "Writing a Prediction Market Contract"
- Chrisjan Pauw "Bitcoin Futures, Explained"
- Bentov, I., Mizrahi, A., and Rosenfeld, M. "Decentralized prediction market without arbiters". In International Conference on Financial Cryptography and Data Security, pp. 199-217.
- Efi Pylarinou. "Are Decentralized Exchanges part of the Bottom-up decentralized monetary policy?"

UNIVERSITY *of* NICOSIA

Instructor’s Email:
iosif.e@unic.ac.cy