Zero-knowledge “proof” for bet anonymity

David Vas
The bet

- When will Jane break up with her boyfriend?
  - Alice: 2018 February
  - Bob: 2018 May
  - Cecilia: 2018 October
  - Jane: WTF guys...
  - ...
  - David: A8E85DA09D43BABB5DE54ED0CC04A745AB25F198A83F1B7E9735043A0D9FB89
The problem with full-knowledge betting

• Betting order matters
• E.g.
  • Alice: 2018-02-27
  • Bob: 2018-03-01
  • Cecilia: 2018-02-26
• “Dirty play” is more likely
Zero-knowledge bets

• Bets want to be anonymous too!
• One-way encryption: share the hash, keep the bet
• “Public key” is your hash that you share with everyone
  • A8E85DA09D43BABBB5DE54ED0CC04A745AB25F198A83F1B7E9735043A0D9FB89 (SHA-256)
• Keep the “private key” (your bet) safeguarded
  • I think Jane will end up marrying her boyfriend.
• Don’t just bet the date or number, “seed” your data (small keyspace is easily brute-forced)
• After the event everyone can verify
• Minimal effort
• Reduced risk for dirty play
Stay tuned for...

• Betting using Smart Contracts on the Ethereum blockchain