## 11.2.2. Teoria gier: Podstawowe pojęcia i definicje

*Gra* składa się ze zbioru *graczy*, zbioru *działań* oraz *strategii* (strategia to sposób, w jaki każdy gracz wybiera działania) oraz z *funkcji użyteczności,* która jest wykorzystywana przez każdego gracza do obliczania korzyści (wielkości wypłaty) uzyskiwanej w przypadku wyboru określonego działania. W *grach kooperacyjnych* gracze współpracują ze sobą i dzielą łączną wypłatę między siebie, czyli do współpracy motywuje ich zbieżność interesów. Z kolei w *grach niekooperacyjnych* gracze nie są w stanie osiągnąć między sobą porozumienia w sprawie koordynacji swoich działań. Innymi słowy, ewentualna współpraca między graczami musi być samoistna. Teraz opiszemy krótko pewne dobrze znane koncepcje z teorii gier [9], które przydadzą się w naszych późniejszych analizach i dyskusji.

**Definicja 1:** Niech $A \stackrel{def}{=} A_1 \times A_2 \times \ldots \times A_n$ będzie profilem działań dla $n$ graczy, gdzie $A_i$ oznacza zbiór możliwych działań gracza $P_i$. Gra $\Gamma = (A_i, u_i)$, dla $1 \leq i \leq n$, składa się z $A_i$ oraz z funkcji użyteczności $u_i : A \rightarrow R$ dla każdego gracza $P_i$. Wektor działań $\vec{a} = (a_1, \ldots, a_n) \in A$ będziemy nazywali *wynikiem gry*.

**Definicja 2:** *Funkcja użyteczności* $u_i$ opisuje preferencje gracza $P_i$ odnośnie różnych wyników. Mówimy, że gracz $P_i$ preferuje wynik $\vec{a}$ nad $\vec{a}'$, jeśli $u_i(\vec{a}) > u_i(\vec{a}')$, oraz że *słabo preferuje* wynik $\vec{a}$ nad $\vec{a}'$, jeśli $u_i(\vec{a}) \geq u_i(\vec{a}')$.

Aby umożliwić graczom działanie według strategii, definiujemy $\sigma_i$ jako rozkład prawdopodobieństwa na $A_i$ dla gracza $P_i$. Oznacza to, że gracz wybiera $a_i \in A_i$ zgodnie ze strategią $\sigma_i$. Mówimy, że strategia jest *czysta,* jeśli każdy $\sigma_i$ przypisuje prawdopodobieństwo 1 określonemu działaniu. Jeśli tak nie jest, mówimy, że strategia jest *strategią mieszaną*. Niech $\vec{\sigma} = (\sigma_1, \ldots, \sigma_n)$ będzie wektorem strategii graczy i niech $(\sigma'_i, \vec{\sigma}_{-i}) = (\sigma_i, \ldots, \sigma_{i-1}, \sigma'_i, \sigma_{i+1}, \ldots, \sigma_n)$, gdzie $P_i$ zastępują $\sigma_i$ przez $\sigma'_i$, a strategie wszystkich pozostałych graczy pozostają niezmienione. Zatem $u_i(\vec{\sigma})$ oznacza oczekiwaną użyteczność $P_i$ pod wektorem strategii $\vec{\sigma}_i$. Celem gracza jest maksymalizacja $u_i(\vec{\sigma})$. W poniższych definicjach działanie $a_i \in A_i$ można zastąpić jego rozkładem prawdopodobieństwa $\sigma_i \in S_i$ i vice versa.

**Definicja 3:** Wektor strategii $\vec{\sigma}_i$ jest w *równowadze Nasha*, jeśli dla wszystkich $i$ oraz dla dowolnego $\sigma'_i \neq \sigma_i$ prawdą jest, że $u_i(\sigma_i, \vec{\sigma}_{-i} \leq u_i(\vec{\sigma}_i)$. Oznacza to, że nikt nie zyskuje żadnej przewagi w wyniku odstępstwa od protokołu, dopóki inni postępują zgodnie z nim.

**Definicja 4:** Niech $S_{-i} \stackrel{def}{=} S_1 \times \ldots \times S_{i-1} \times S_{i+1} \times \ldots \times S_n$. Strategia $\sigma_i \in S_i$ (lub działanie) jest *słabo zdominowana* przez $\sigma'_i \in S_i$ (lub inne działanie) pod względem $S_{-i}$, jeśli dla każdego $\vec{\sigma}_{-i} \epsilon S_{-i}$, spełniona jest zależność: $u_i(\sigma_i, \vec{\sigma}_{-i}) \leq u_i(\sigma'_i, \vec{\sigma}_{-i})$. Istnieje $\vec{\sigma}_{-i} \epsilon S_{-i}$ taka, że $u_i(\sigma_i, \vec{\sigma}_{-i}) < u_i(\sigma'_i, \vec{\sigma}_{-i})$. Oznacza to, że gracz $P_i$ nie może nigdy poprawić swojej

użyteczności, wybierając strategię $\sigma_i$, oraz że czasami może ją poprawić, nie wybierając strategii $\sigma_i$. Strategia $\sigma_i \in S_i$ jest *ściśle zdominowana*, jeśli gracz $P_i$ zawsze może poprawić swoją użyteczność, nie wybierając strategii $\sigma_i$.

## 11.3. Przegląd literatury

Koncepcja blockchaina jest stosunkowo młoda, gdyż została zaprezentowana przez nieznanego autora lub autorów w 2008 roku. Mimo to zdobyła już znaczne uznanie społeczności informatycznej i ekonomicznej ze względu na swoje wyjątkowe podejście do kwestii decentralizacji weryfikacji transakcji związanych z cyfrowymi walutami i za sprawą jej naturalnego bezpieczeństwa, wynikającego z jej zdecentralizowanej natury. Jednak istnieje stosunkowo niewiele prac poświęconych badaniom blockchainów metodami teoretycznymi. W tym podrozdziale przedstawimy przegląd prac badawczych poświęconych blockchainowi w ujęciu teorii gier.

Autorzy pracy [6] – Johnson i inni – badają motywacje spółdzielni wydobywczych do przeprowadzenia ataków typu *distributed denial-of-service* (DDoS) na inną spółdzielnie wydobywczą. Analizują oni to zagadnienie z ekonomicznego punktu widzenia, zakładając że motywacją do ataku jest zwiększenie prawdopodobieństwa pomyślnej weryfikacji następnego bloku transakcji atakującego, a tym samym zdobycie wynagrodzenia w Bitcoinach za jego wydobycie. Autorzy tej pracy dochodzą do wniosku, że motywacja do atakowania dużych spółdzielni wydobywczych jest większa niż motywacja do atakowania małych. Zwracają uwagę, że wnioski te są zgodne ze statystykami przedstawionymi w pracy [10], według których ofiarą ataków DDoS padło 17,1% małych spółdzielni wydobywczych i że w przypadku dużych spółdzielni ataki takie dotknęły aż 62,5% z nich. Autorzy czynią również kolejne dwie interesujące obserwacje. Po pierwsze, zdolność radzenia sobie z atakami DDoS będzie zwiększać próg rynkowy, po przekroczeniu którego spółdzielnia staje się podatna na ataki DDoS. Wydaje się to być intuicyjnym wnioskiem, ponieważ zdolność do radzenia sobie z takimi atakami zmniejsza wartość funkcji użyteczności atakującego. Po drugie, koszt ataków DDoS sprawia, że małe spółdzielnie nie stają się ich celem, ponieważ korzyści z atakowania ich są stosunkowo małe.

Babaioff i in. [11] analizują inny problem występujący w protokole Bitcoin. Problem ten nasili się, gdy zakończy się wypłacanie wynagrodzenia za wydobycie bloków w sieci Bitcoin. Obecnie węzły weryfikujące transakcje otrzymują dwojakie wynagrodzenie. Po pierwsze, otrzymują nowo emitowane Bitcoiny za dołączenie każdego nowego bloku do łańcucha, a po drugie – otrzymują opłaty transakcyjne od użytkowników.

Maksymalna liczba Bitcoinów w obiegu jest sztywno ograniczona do około 21 milionów [12]. Emisja nowych Bitcoinów będzie cały czas wykładniczo maleć aż do osiągnięcia maksymalnej liczby monet w obiegu. Po osiągnięciu tego maksymalnego progu, opłata transakcyjna stanie się jedynym źródłem wynagrodzeń dla górników. Górnicy będą wówczas mieć motywację do ukrywania informacji o potencjalnych transakcjach, ponieważ praca poświęcona na dołączanie bloków do łańcucha nie będzie wynagradzana nowo emitowanymi bitcoinami, czyli weryfikator transakcji będzie otrzymywał wyłącznie opłatę transakcyjną. Motywacja do utajniania tych informacji może potencjalnie osłabić system Bitcoin, ponieważ czas potwierdzenia transakcji wydłuży się, gdy transakcja będzie weryfikowana przez tylko jeden węzeł.

Kroll i in. [13] badali sieć Bitcoin jako grę konsensusową i rozważali ekonomikę wydobycia bitcoinów. Ich celem było ustalenie motywacji dla racjonalnych graczy do nieprzestrzegania protokołu wydobycia. Autorzy pracy dowodzą w niej, że istnieje pewien wynik w równowadze Nasha, w przypadku którego wszyscy gracze współpracują zgodnie z referencyjną implementacją Bitcoina. Istnieje jednak nieskończenie wiele punktów równowagi, w których gracze mogą zachowywać się inaczej. Autorzy pokazują, że zmotywowany przeciwnik może być w stanie wykonać udany atak na tę kryptowalutę i że w związku z tym wymagane będzie wprowadzenie struktur zapewniających ład.

Barber i in. [14] nie odwołują się do żadnych modeli z teorii gier. Opisują natomiast kilka potencjalnych możliwych luk w protokole blockchaina, które doskonale nadają się do rozważań w kontekście teorii gier. Są to: spirala deflacyjna, atak zmiany historii oraz opóźnione potwierdzanie transakcji. Carlsten i in. [15] analizują problemy Bitcoina i jego blockchaina, które pojawią się po wypłaceniu górnikom ostatniego wynagrodzenia za blok. Autorzy pokazują, że gdy zakończy się wypłacanie wynagrodzeń za wydobycie i pozostaną jedynie opłaty transakcyjne, zwiększy się motywacja do działań przeciwko protokołowi.

Luu i in. [16] analizują atak wstrzymywania bloków na spółdzielnie wydobywcze, opisany po raz pierwszy przez Rosenfelda [4]. Dowodzą, że w długiej perspektywie zawsze istnieje motywacja do tego ataku, ale może on być nieopłacalny w perspektywie krótkoterminowej. Analizując to samo zagadnienie, Eyal [17] dochodzi do wniosku, że gdy dwie spółdzielnie atakują się nawzajem, w rezultacie występuje rodzaj dylematu więźnia, który nazywa się *dylematem górnika*. Lewenberg i in. [18] wprowadzają modyfikację protokołu Blockchain, która umożliwia włączanie bloków z rozwidleń w celu przyspieszenia działania sieci. Następnie przedstawiają oparty na teorii gier model rywalizacji węzłów stosujących nowy protokół o wynagrodzenia.