Eter jednak istnieje!

Naturalnie, wszystko się zaczyna od *tabula rasa.*

Toteż załóżmy, że dysponujemy wielką niezapisaną tablicą. Po tej tablicy pisać będzie mógł absolutnie każdy, kto tylko chce. Pisać wolno wszystko, należy się jedynie podpisywać. Komunikaty nigdy nie znikają, a budowa tablicy jest taka, że łatwo się zorientować, w jakiej kolejności pojawiały się obecne na niej napisy.

Taka tablica jak wyżej, wyeksponowana gdzieś na *Forum Romanum*, może już posłużyć do stworzenia systemu bankowego, opartego o własną nową walutę tablicową $\mathbb{T}$. Umawiamy się tylko, że raz na pół godziny publicznie losujemy obywatela X i zapisujemy komisyjnie na tablicy napis:

„Obywatel X wylosował 1$\mathbb{T}$”, podpisano: Komisja.

Jako się rzekło, każdy może pisać co chce, ale przede wszystkim zapisuje się przelewy. Oto przykład kilku kolejnych możliwych komunikatów zapisanych na tablicy:

1. „Obywatel A wylosował 1$\mathbb{T}$”, podpisano: Komisja.
2. „A przelewa do B 0,5$\mathbb{T}$”, podpisano: A.
3. „Obywatel A wylosował 1$\mathbb{T}$”, podpisano: Komisja.
4. „A przelewa do C 1,5$\mathbb{T}$”, podpisano: A.
5. „C przelewa do D 1$\mathbb{T}$”, podpisano: C.
6. „Obywatel E wylosował 1$\mathbb{T}$”, podpisano: Komisja.

Wszystko powyżej wygląda w porządku, ale przecież tablica mogłaby wyglądać również, na przykład, tak:

1. „Obywatel A wylosował 1$\mathbb{T}$”, podpisano: Komisja.
2. „A przelewa do B 0,5$\mathbb{T}$”, podpisano: A.
3. „A przelewa do C 1$\mathbb{T}$”, podpisano: A.
4. „Obywatel B wylosował 1$\mathbb{T}$”, podpisano: Komisja.
5. „B przelewa do C 1$\mathbb{T}$”, podpis: niewyraźny.

W takiej sytuacji dla każdego członka społeczności jest jasne, że należy zignorować napis trzeci (A próbuje przelać pieniądze, których nie ma) oraz napis piąty (nie jest poprawnie podpisany), a obywatele A, B i C dysponują odpowiednio 0,5$\mathbb{T}$, 1,5$\mathbb{T}$, 0$\mathbb{T}$.

Pomysł, aby waluta działająca tak jak wyżej, była wykorzystywana do codziennych opłat za zakupy czy usługi, wydaje się bardzo podejrzany. Przede wszystkim zaskakuje to, że pieniądze pojawiają się trochę znikąd – w drodze losowania. Po drugie, historia wszystkich transakcji jest publicznie znana. A jednak! Takie rozwiązanie istnieje w naszym świecie i nazywa się Bitcoin. Oczywiście, z jednej strony można argumentować, że przecież nie ma w tym nic aż tak ekonomicznie szokującego. Przez setki lat walutą były przecież różne szlachetne kruszce, które mają bardzo podobne właściwości jak nasze $\mathbb{T}$ – znajdujemy je rzadko i dość losowo, same w sobie nie mają wielkiej bezpośredniej wartości, a jednak istnieją osoby o zdrowych zmysłach, które są w stanie np. wymienić swój własny dom na kilka kilogramów żółtawego, błyszczącego metalu. Mimo to wciąż może szokować, że istnieją osoby (również o zdrowych zmysłach), które są w stanie oddać ten szlachetny kruszec za wpis na dziwnej publicznej tablicy od osoby, która np. właśnie wylosowała bitcoina.

Dla porządku napiszmy, że w świecie Bitcoina nie mówimy o publicznej tablicy, a o *blockchainie* (łańcuchu blokowym). Spełnia on tę samą rolę, ale jego stworzenie nie jest wcale łatwe.

(Jedna rzecz jest nawet lepsza. W Bitcoinie łatwo jest się ukryć za cyfrowym pseudonimem. Pełnej anonimowości więc, oczywiście, tutaj nie ma, ale jest tzw. pseudonimowość.)

Oczywiście, byłoby ono zupełnie trywialne, gdybyśmy założyli istnienie jednej zaufanej strony, która wszystko uczciwie zapisuje, losuje, nie dodrukowuje sobie pieniędzy i generalnie dba, żeby hajs się zgadzał. My, ze względów na bezpieczeństwo i słabość do anarchii, chcemy jednak, żeby system był rozproszony. Co to znaczy i jak to jest zrobione technicznie, opisał już w *Delcie* 6/2016 Łukasz Mazurek. Dalej będziemy zakładać, że bezpieczną tablicę (pardon, blockchain) po prostu mamy dostępną. Zastanówmy się, jakie (inne niż przelewy) napisy na tej tablicy mogłyby być użyteczne. Oto przykłady:

...
130. „A przelewa 1$\mathbb{T}$ pierwszej osobie, która poda rozkład na czynniki pierwsze liczby 681148087”, podpisano: A. 131. „C przelewa do D 10$\mathbb{T}$, jeśli Jagiellonia Białystok zostanie mistrzem Polski w piłce nożnej w sezonie 2017/18.”, podpisano: C. 132. „681148087 rozkłada się na 21739 i 31333”, podpisano: B.

W roku 2015 Witalik Buterin stworzył nową walutę Ethereum (czasem zwaną Bitcoinem 2.0) opartą o blockchain, który umożliwia łatwe tworzenie i realizowanie właśnie tego typu zobowiązań, tutaj zwanych *inteligentnymi kontraktami* (smart contracts), zapisanych w wygodnym języku Solidity. Oto przykład takiego kontraktu (autor niniejszego felietonu zobaczył go kiedyś w prezentacji Daniela Malinowskiego i Łukasza Mazurka):

```
contract Factor
{ function factor681148087 (uint p, uint q)
  { if (p > 1 && q > 1)
        && (p * q == 681148087))
    { msg.sender.send(1 ether); }
  }
}
```

Przykład powyżej może wydać się trochę akademicki, jednak Ethereum naprawdę ma ogromny praktyczny potencjał. Informatycy już pokazali, jak zrobić na jego bazie choćby rozproszony system do gier hazardowych typu poker (oparty tylko o – publiczny przecież! – blockchain). Ale to już temat na inną opowieść...

Tomasz KAZANA