그래서, 블록체인이 뭔데? (WTF is blockchain?)

2018년 11월 24일 토요일 오후 8:56

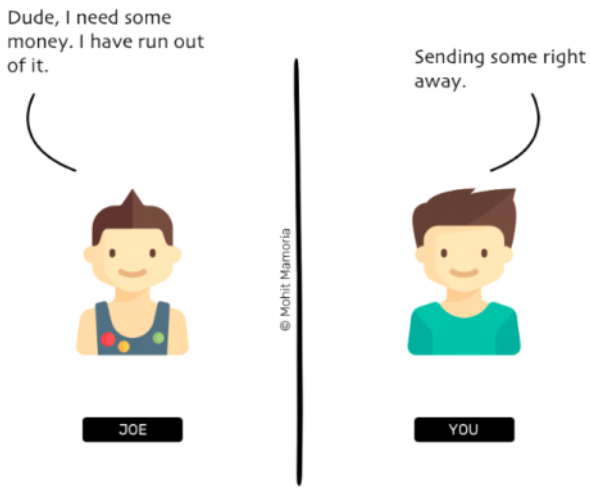
블록체인 : 우리는 왜 이렇게 복잡한 것을 필요로 할까요?

"모든 복잡한 문제에 대해 명확하고 단순하며, 잘못된 답이 있습니다."

— H.L. 멘켄 (미국의 저널리스트)

인터넷에 올라온 대부분의 블록체인 관련 글과 다르게, 저는 블록체인에 대해서 먼저 정의하기 이전에 '그것이 해결하는 문제'에 대해서 먼저 이야기해보겠습니다.

당신에게 지금 해외여행 중인 '조'라는 친한 친구가 있다고 가정해 봅시다. 조가 휴가간지 5일째 되는 날 당신에게 "나 돈이 떨어졌는데 돈 좀 꿔줘."라고 연락을 합니다. 당신은 조에게 "곧 돈 보낼게, 조금만 기다려."라고 말하고 전화를 끊습니다.



당신은 조의 전화를 끊고, 은행의 계좌 담당자에게 전화를 걸어 "내 계좌에서 조의 계좌로 천 달러를 이체해주세요."라고 요청하고, 담당자는 그에 대해서 그러겠다고 답변합니다. 그는 계좌를 조회해 천 달러 이상의 잔액이 있는지 확인합니다. 여러분이 넉넉한 잔액을 갖고 있기 때문에, 담당자는 'OK'하고 당신이 조의 계좌로 빌려준 내역을 기록합니다.

그리고, 당신은 조에게 전화해서 "돈을 이체했으니 나중에 은행에 가서 내가 방금 송금한 천 달러 인출해."라고 전합니다.

자, 지금까지 무슨 일이 일어났나요? 당신과 조는 모두 당신의 돈을 관리하고 있는 은행을 믿었습니다. 이 과정에서 '실제'로 오간 '현찰'은 없었습니다. 필요한 것은 등록부에 해당 이체내역을 기록한 것 뿐입니다. 더 정확히 말하면, 기록된 항목은 당신과 조가 컨트롤하거나 소유하지 못하는 것입니다.

이것이 바로, 현재 시스템의 문제입니다.

"우리 사이에 신뢰를 구축하기 위해, 우리는 '각각 개별적인' 제 3자에 의존한다."

몇년 동안, 우리는 이러한 중개인(은행)들에게 의존하여 서로에게 믿음을 다져 왔습니다. 여러분은 "그것을 다루는데 어떠한 문제가 있나요?"라고 물어볼 수 있습니다.

문제는 그들이 수적으로 열세라는 것입니다. 만약, 사회에 혼란스러운 상황이 주입되어야 한다고 가정하면, 의도적으로 혹은 의도적이지 않게 부패된 사람/조직이 필요합니다.

– 만약 은행에 불이 나서 당신과 조와의 거래 내역이 기록된 장부가 불에 탄다면?

– 은행 계좌 관리자가 천 달러가 아닌 천 오백 달러를 송금했다면?

– 관리자가 일부러 실수를 저질렀다면?

"몇년 동안, 우리는 우리의 모든 달걀을 한 바구니에 담아 왔고, 다른 누군가의 바구니에도 똑같이 넣어 왔다"

과연 은행 없이도 돈을 송금할 수 있는 시스템이 존재할 수 있을까요?

이 질문에 대답하기 위해, 우리는 이 문제에 대해 조금 더 깊이 파고들어서 스스로에게 물음을 던질 필요가 있습니다.

잠깐 생각해 보세요. 돈을 송금하는 것이 무엇을 뜻하는 걸까요? 그냥 장부에 기입하는 것? 더 나은 고민은 거기에서 나올 것입니다.

"다른 사람이 우리를 위해 거래 내역 등록을 대행하는 방법 이외에, 우리 사이에 등록을 유지할 수 있는 또 다른 방법이 있을까?"

자, 이것은 깊이 생각해 볼 만한 가치가 있는 질문입니다. 그리고 그에 대한 답변은 여러분이 생각했던 그대로입니다. 블록체인이 위의 질문에 대한 답이 될 수 있습니다. 블록체인은 그것을 '다른 누군가에게 의존'하는 대신에 '우리들 사이'에 등록을 유지할 수 있는 방법입니다.

이제 조금씩 이해가 되시나요? 좋습니다. 여러분의 머릿속에 몇 가지 의문점이 떠오르기 시작하면, 우리는 이 블록체인이라는 등록 방법이 어떤 식으로 작동하는 지 알 수 있을 겁니다.

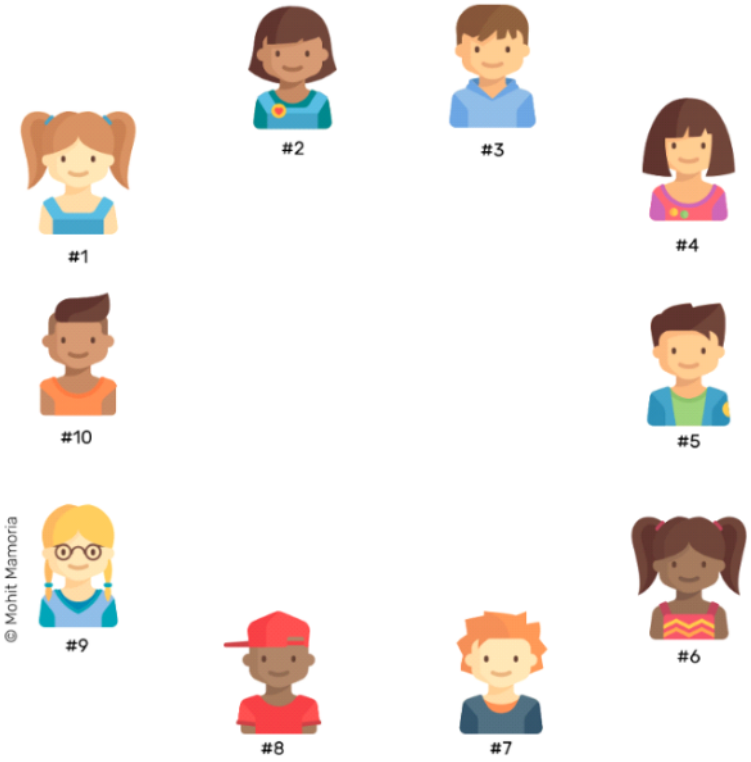
좋아요. 블록체인은 어떻게 움직이나요?

이 방법의 필수적인 선행 조건은 당신과 같이 **제 3자에게 의존하지 않으려는 사람들의 수가 충분해야 한다는 것**입니다. 그래야만 이 사람들의 모임이 자체적으로 '등록 방법'을 관리할 수 있습니다.

"만약 비트코인이 유행할 경우를 대비해, 비트코인을 구입하는 것은 의미가 있습니다. 많은 사람들이 이와 같은 생각을 갖고 있다면, 그것은 '자기 충족적 예언'이 될 것입니다."

— 2009년, 나카모토 사토시(비트코인 개발자)

몇 명이면 충분할까요? 적어도 세 명은 필요합니다. 예를 들어, 10명의 사람들이 은행이나 제 3자에 대해서 필요없다 생각한다고 가정해봅시다. 상호 합의에 따라, 그들은 서로 다른 사람의 신원에 대해 모른 채 서로의 계좌에 대한 세부 내용을 알고 있습니다.



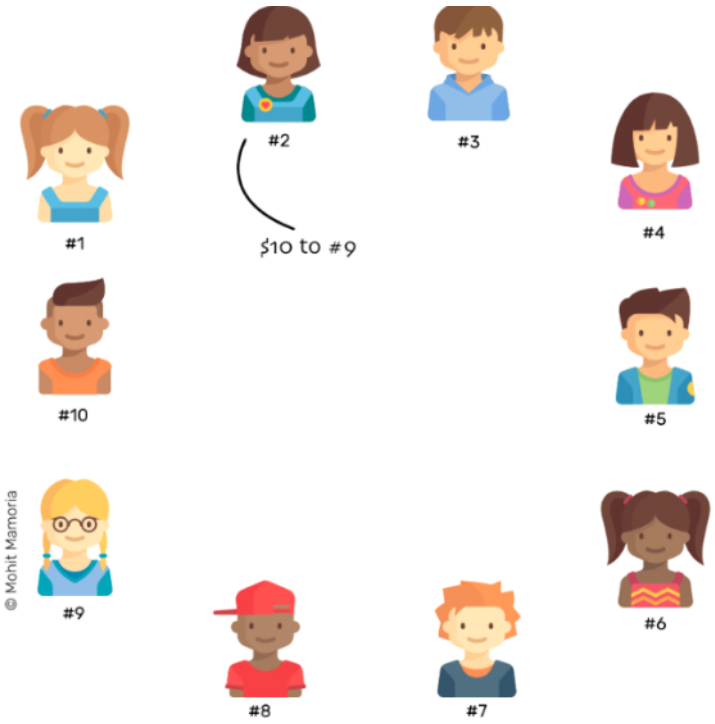
1. 비어있는 폴더

처음에는 빈 폴더만 있으면 됩니다. 이 10명의 사람들은 모두 현재 비어 있는 폴더에 페이지를 계속 추가할 것입니다. 그리고 이 페이지 모음은 거래 과정을 추적하는 레지스터를 형성할 것입니다.

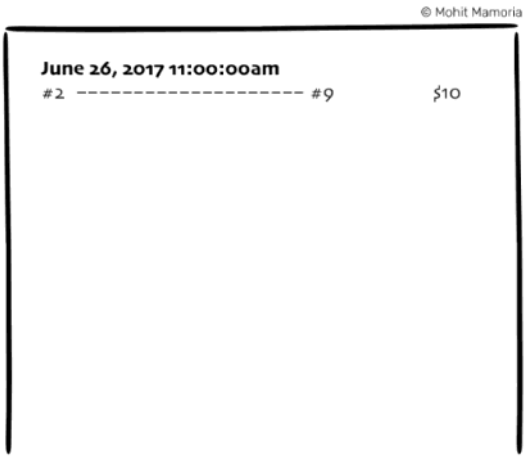
2. 거래가 발생했을 때

네트워크에 있는 모든 사람들은 빈 페이지와 펜을 손에 들고 있으며, 시스템 내에서 발생하는 모든 거래 내역에 대해 작성할 수 있습니다.

2번 사람이 9번 사람에게 10달러를 보내고 싶다면, 2번 사람은 송금을 위해, 모든 사람들에게 소리 치면서, “제가 지금 9번 사람에게 10달러를 보낼거예요. 그러니, 여러분 모두 이것을 여러분의 페이지에 적어 두세요.” 라고 말합니다.



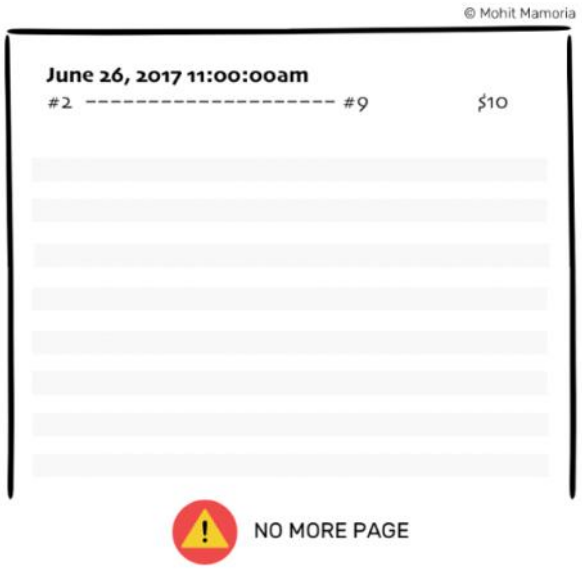
2번 사람이 9번 사람에게 10달러를 보내기 위해 충분한 잔고가 있는지 모든 사람들이 확인하고, 계좌 잔고가 충분하다고 확인되면 모든 사람들이 자신의 빈 페이지에 해당 거래 내역을 기록합니다. 이 과정을 거치면, 거래가 완료된 것으로 간주합니다.



3. 거래가 계속 이루어질 때

시간이 흐르면, 네트워크 내의 많은 사람들이 다른 사람들에게 돈을 보낼 필요성을 느끼게 됩니다. 거래를 할 때마다, 그것을 다른 모든 사람들에게 알리고, 똑같이 페이지에 내역을 기록합니다.

이 과정은 페이지 내 빈 공간이 없어질 때까지 계속됩니다. 한 페이지에 10개의 거래내역을 기록할 수 있는 공간이 있다면, 10번 째의 거래 내역이 기록되는 순간, 모든 사용자는 거래 내역을 기록할 공간이 부족해집니다.



이제 페이지를 폴더에 넣고 새 페이지를 꺼내서 위의 두 단계에서 설명한 과정을 반복해야 합니다.

4. 페이지의 보관

페이지를 폴더에 넣기 전에, 그것을 네트워크 상의 모든 사람들이 동의하는 고유한 열쇠로 봉인해야 합니다. 그것을 봉인함으로써, 우리는 복사본이 모두의 폴더에 넣어진 후에, 그 누구도 변경할 수 없도록 할 것입니다. 폴더에 넣으면 언제까지라도 항상 폴더 안에 보존된 상태로 남아 있게 됩니다. 뿐만 아니라 모두가 그 열쇠를 신뢰하는 경우에는 페이지에 기록된 내용도 신뢰하게 됩니다. 따라서, 이 페이지를 봉인하는 것이 이 방법의 가장 핵심입니다.

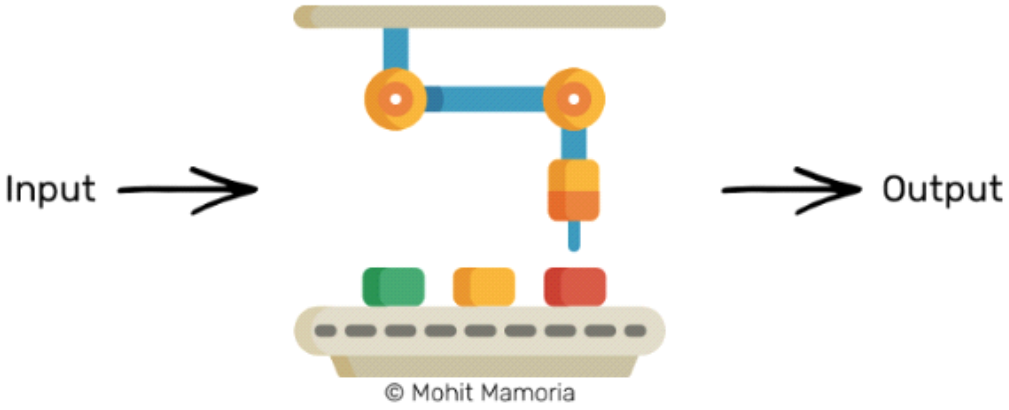
이전에 제 3자나 중개인은 우리에게 그들이 장부에 적은 것은 절대 변경되지 않을 것이라는 신뢰를 주었습니다. 위와 같은 분산되고 분권화된 시스템에서는 '봉인한 열쇠'가 대신 신뢰를 주는 도구가 될 것입니다.

거참 재미있네요. 그럼 페이지는 어떻게 봉인하나요?

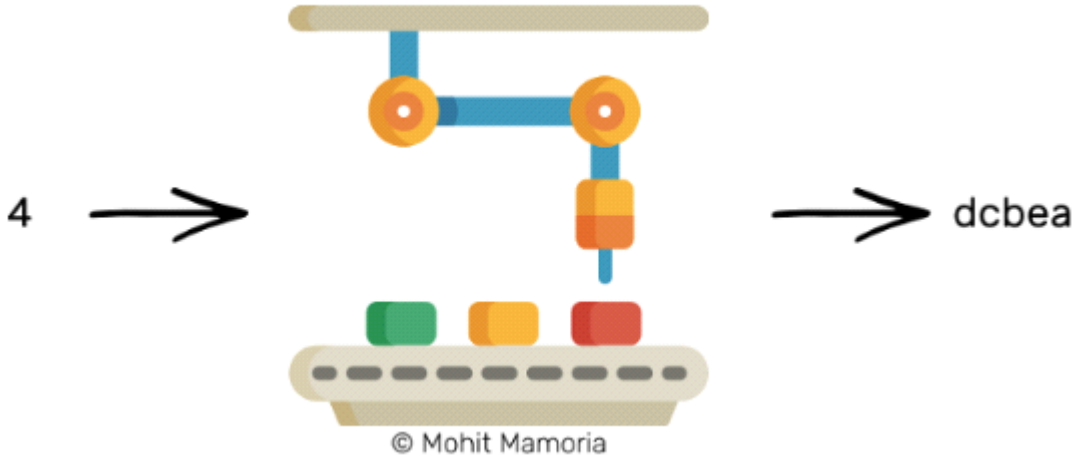
그 페이지를 어떻게 봉인하는지 알아내기 전에, 일반적으로 우리는 봉인이 어떻게 작동하는지 알아야 합니다. 제가 해당 개념에 대해서 설명하기 위해 가정한 것들에 대한 이해가 필요합니다.

1. 마법 기계

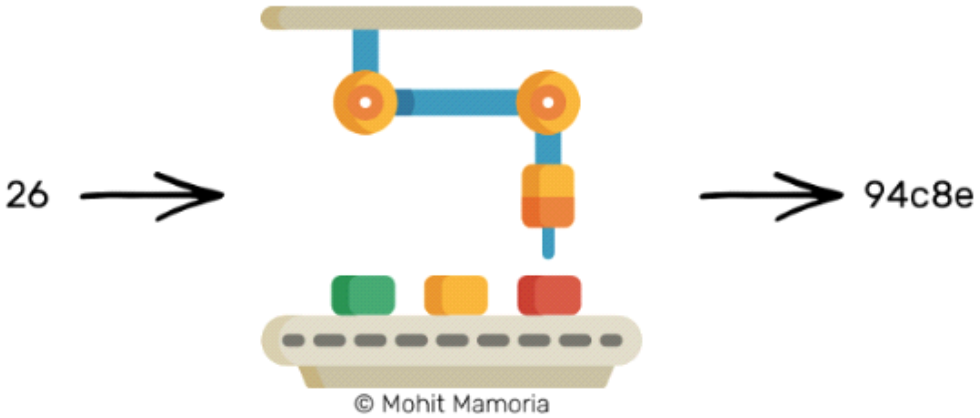
두꺼운 벽으로 둘러싸인 기계를 상상해 보세요. 이것은 실제로는 '해시 함수 (Hash Function)'라고 부르지만 여기에선 마법 기계라고 칭하도록 하겠습니다. 만약 당신이 왼쪽 방향에서 무언가가 들어있는 상자를 보낸다면, 그 기계는 또 다른 것이 들어있는 상자를 뱉어낼 것입니다.



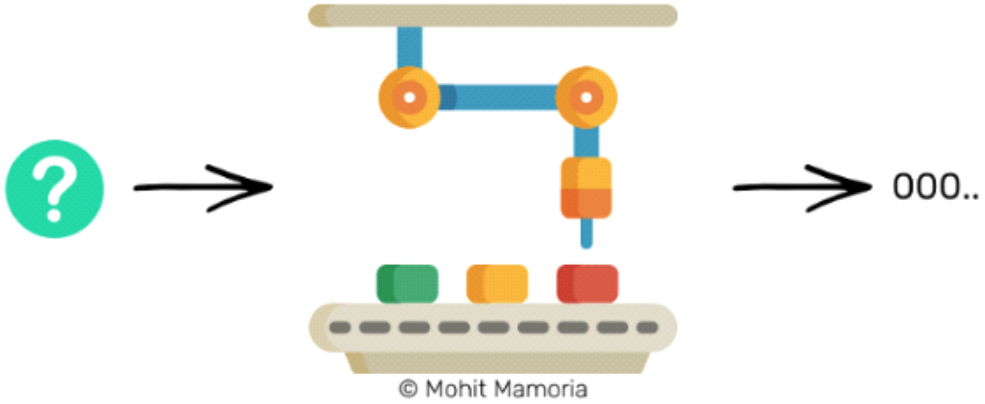
예를 들어 기계를 통해 왼쪽에서 숫자 4를 보내면, 오른쪽에 'dcbea'라는 단어가 나온다고 해 봅시다. 숫자 4가 어떻게 dcbea라는 단어로 바뀌었을까요? 아무도 모를 뿐더러, 돌이킬수 조차 없습니다. **왼쪽에서 무엇을 넣으면 dcbea라는 단어가 나오는지 추론해 내는 것은 불가능합니다.** 다만, 4번을 입력할 때마다 항상 dcbea라는 단어를 뱉어냅니다.



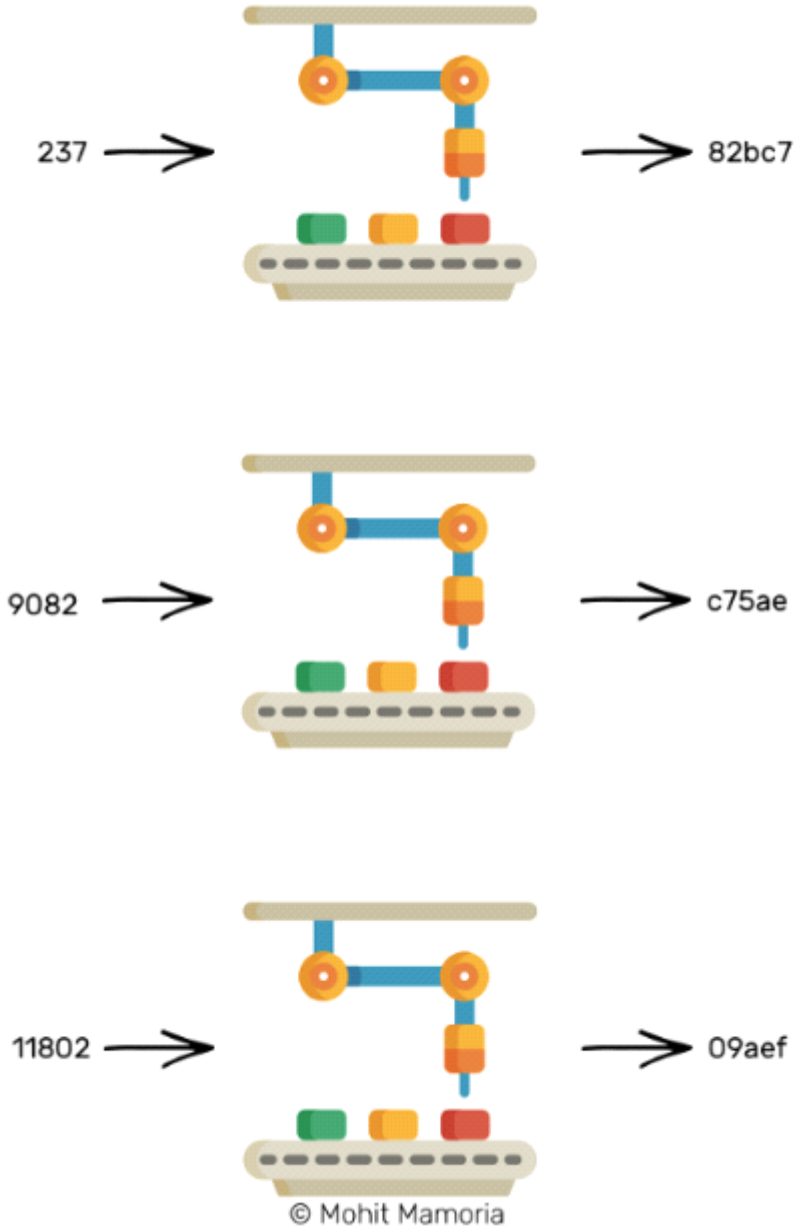
26번이라는 다른 번호를 기계에 넣어 볼까요? 이번에는 94c8e라는 단어가 나왔습니다. 어라, 숫자도 입력이 가능하네요? 단어 배열에는 숫자도 들어갈 수 있습니다.



이제 다음과 같은 질문을 해 보겠습니다. "오른쪽에서 000ab, 00098, 000fa 등 000으로 시작되는 단어의 조합을 얻으려면, 왼쪽에서 어떠한 숫자를 보내야 합니까?"



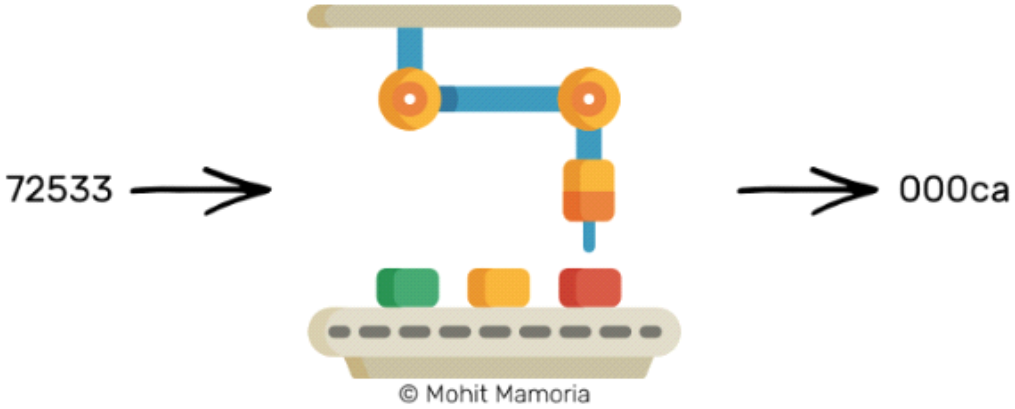
이 질문에 대해 잠시 생각해 봅시다.이미 위에서 왼쪽으로부터 보낸 단어로 오른쪽의 결과값으로 옮겨진 과정을 계산할 수 없다는 것을 이야기했습니다. 이런 기계가 우리에게 주어진다면, 위의 질문에 어떻게 대답할 수 있을까요?



저는 한가지 방법을 생각해 봤습니다. “왜 000으로 시작하는 조합의 단어가 나타날 때까지 모든 숫자들을 하나하나 입력해볼 생각을 하지 않았을까?” 아무 생각 없이 수천 번의 시도를 해 나가다 보면 오른쪽에 원하는 값을 얻을 수 있을 것입니다.

출력을 계산해 나가는 과정은 매우 어렵지만 기계는 매번 같은 단어를 숫자로 나타낸다는 점을 기억한다면, 예측되는 입력값이 필요한 결과값을 뽑아 내는지의 여부를 확인하는 것은 매우 쉽습니다.

만약 제가 여러분에게 “72533이라는 숫자를 기계 왼쪽에 입력하면, 000으로 시작하는 단어를 뽑아낼 수 있나요?” 라고 묻는다면, 그 대답은 얼마나 어려울 것이라고 생각하십니까? 여러분이 해야 할 일은 숫자를 기계에 입력하고 그 오른쪽에 무엇이 나오는지 확인하는 것 뿐입니다.



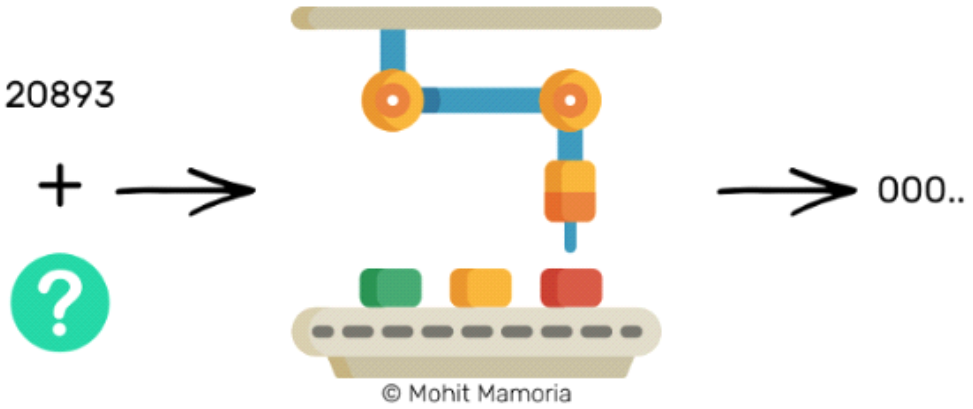
이러한 기계의 중요한 특성은 다음과 같습니다. **“출력으로 입력값을 계산하는 것은 매우 어렵지만, 입력값과 출력값이 주어지면, 입력이 출력으로 이어지는지의 여부를 확인하는 것은 매우 쉽습니다.”**

뒤에 이어지는 내용을 통해 위에 나타난 마법 기계(해시 함수)의 속성을 다시 한번 강조할 것입니다.

2. 이 마법 기계를 사용하여 페이지를 어떻게 봉인할 수 있나요?

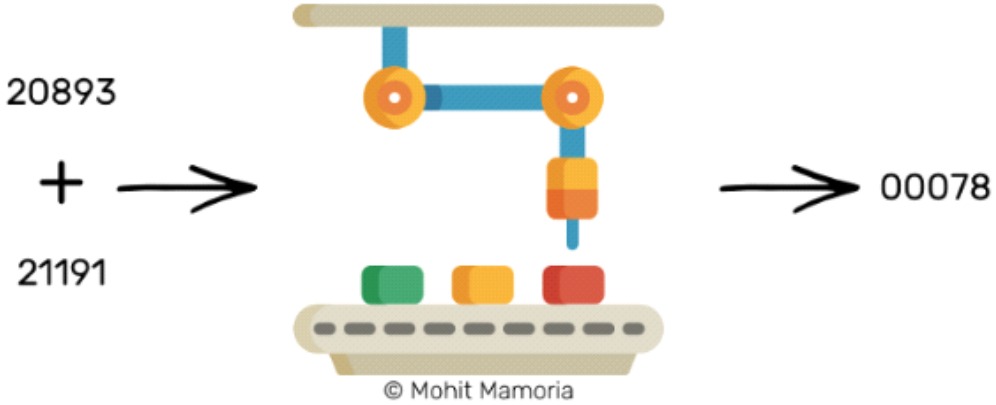
위의 마법 기계를 사용해서 페이지를 봉인해 보겠습니다. 언제나 그랬듯이, 모든 상황은 우리의 상상 속에서 이루어집니다.

제가 당신에게 두 박스를 드릴 것입니다. 그 중 첫번째 박스는 20893번입니다. 그러면 저는 이렇게 물어봅니다. “첫번째 상자의 숫자에 어떤 숫자를 더해야만 000으로 시작하는 단어의 조합이 나올 수 있을까요?”



이러한 숫자를 계산해 내는 유일한 방법은 1번 항목에서 알 수 있듯이 모든 숫자를 일일히 입력해보는 것 뿐입니다.

수천 번의 시도를 해서, 우리는 21191이라는 숫자를 얻어냅니다. 20893에 21191이 더해지면 (21191+20893= 42084) 000으로 시작되는 00078이라는 원하는 단어의 조합이 나옵니다.



이 경우, 21191이라는 숫자는 20893번의 '열쇠'가 됩니다. 페이지에 20893이라는 숫자가 적혀있다고 가정해봅니다. 아무도 이 페이지를 변경할 수 없게 이 페이지를 봉인하려면, 페이지 상단에 21191이라는 인장을 찍습니다. 봉인 번호(즉, 21191)가 페이지에 고정되는 즉시 페이지는 봉인됩니다.

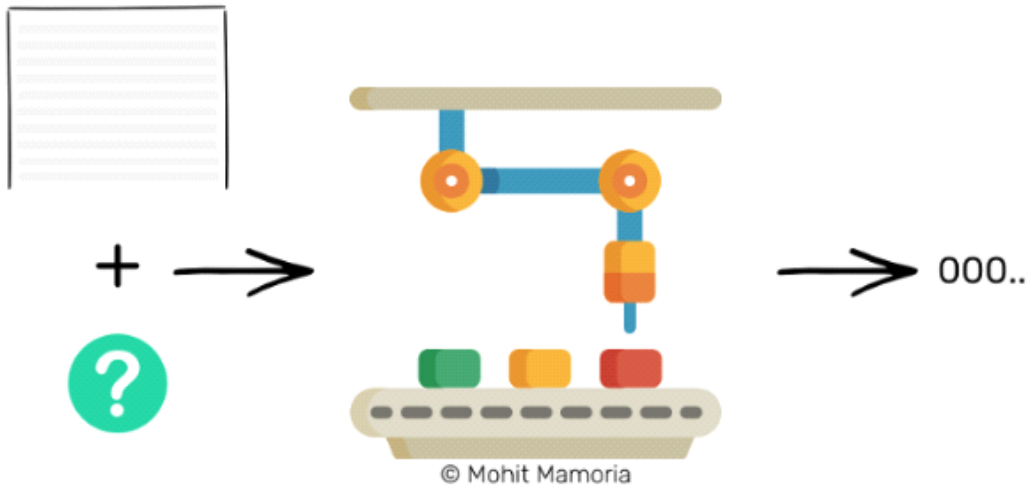
봉인 번호는 '작업 증명(Proof Of Work)'이라고 불리며, 이것은 이 숫자를 계산하기 위해 노력했다는 사실을 의미합니다.

누군가 페이지가 변경되었다는 내용을 확인하고 싶으면, 페이지의 내용에 봉인 번호를 추가하고 마법 기계에 넣으면 끝입니다. 기계를 통해 000으로 시작되는 단어 조합이 나온다면, 내용은 변하지 않습니다. 만약, 나온 단어가 우리가 제시한 조건을 충족시키지 못하면 페이지의 내용이 손상되어 쓸모가 없어지기 때문에 페이지 자체를 버릴 수 있습니다.

우리는 유사한 봉인 메커니즘을 사용해서 모든 페이지를 봉인하고 결국에는 각각의 폴더에 정리할 수 있게 됩니다.

3. 마지막으로, 우리의 페이지를 봉인하는 것

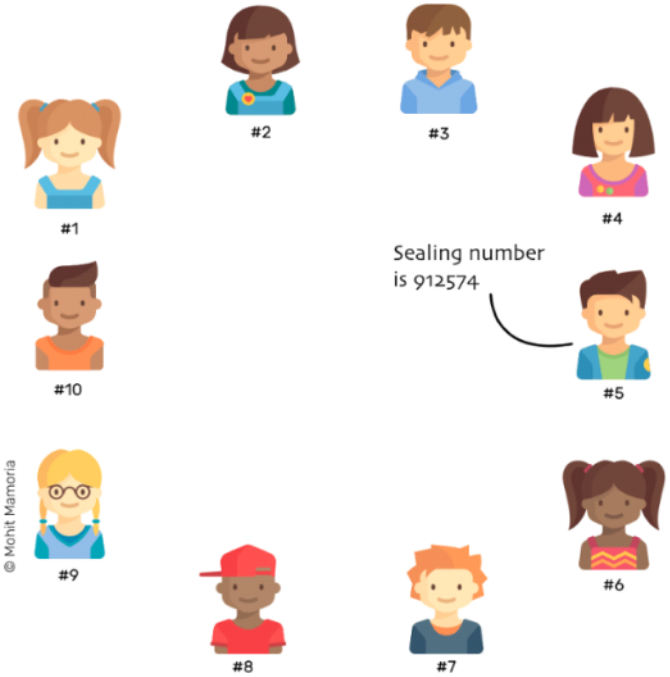
네트워크의 거래 내역이 포함된 페이지를 봉인하려면 거래 내역 목록에 추가되어 기계에 넣어질 때, 오른쪽에 000으로 시작되는 단어가 표시되는지 확인해야 합니다. (사실 000으로 시작되는 단어는 해당 함수의 동작을 설명하기 위한 예제일 뿐, 실제 동작은 비교할 수 없을 만큼 복잡합니다)



일단 그 숫자가 기계에서 시간과 전기를 소비한 후에 계산되고 나면, 그 숫자로 페이지는 봉인됩니다. 어떤 사람이 페이지 내용을 변경하려고 하는 경우, 누구나 봉인 번호를 사용하여 페이지의 무결성을 확인할 수 있습니다.

이제 페이지를 닫는 것에 대해 알았으니 페이지에 10번째 거래를 끝내고 나서 더 쓸 공간이 부족해 진 상황으로 돌아가 보겠습니다.

모든 사람들이 더 많은 거래 내역을 작성하기 위해 페이지를 다 쓰자마자 페이지의 봉인 번호를 계산해서 폴더에 넣을 수 있습니다. 네트워크의 모든 사람이 이것을 알아내기 위해서 계산에 집중합니다. 가장 먼저 봉인 번호를 알아내는 사람이 다른 사람에게 알립니다.



봉인 번호를 듣는 즉시, 모든 사람들이 필요한 결과값이 나오는 지 확인합니다. 만약 들어맞는다면, 모든 사람들은 그들의 페이지에 해당 숫자를 적어서 그들 각각의 폴더에 넣습니다.

그런데, **예를 들어 7번 사람이 봉인 번호를 사용해 필요한 결과값을 얻지 못했다면 어떻게 될까요?** 이러한 결과는 종종 일어납니다. 그 원인은 다음과 같을 수 있습니다.

- 그는 네트워크에서 일어난 거래 내용을 잘못 들었을 수도 있다

- 그가 네트워크에서 일어난 거래 내용을 페이지에 잘못 썼을 수 있다

- 그는 자신이나 네트워크 상의 다른 사람에게 잘 보이기 위해, 부정 행위를 하거나

거래 내용을 쓸 때 정직하지 못한 행동을 했을 수 있다

이유야 어쨌든간에, 7번 사람은 한가지 선택권만 가질 수 있습니다. 그것은 그의 페이지를 버리고 폴더에 넣을 수 있도록 다른 사람으로부터 페이지를 복사하는 것입니다. 그가 그의 페이지를 폴더에 넣지 않는 한, 그는 더 이상의 거래 내역을 기록할 수 없기 때문에, 그는 네트워크의 구성원으로 남아있을 수 없습니다.

"대다수가 동의하는 모든 봉인 번호는 정직한 봉인 번호가 됩니다"

그러면 사람들은 다른 누군가가 계산해서 봉인 번호를 알려줄 것이라는 것을 알면서도 계산을 하는데 시간과 노력을 쏟는 것일까요? 그냥 앉아서 발표를 기다리는 게 낫지 않을까요?라는 의문이 들 수 있습니다.

좋은 질문입니다. 여기에서 우리는 '인센티브'라는 것에 주목해야 합니다. 블록체인 네트워크에 참여하는 사람들은 모두 보상을 받을 수 있습니다. 첫 번째로 봉인 번호를 풀어내는 사람은 자신의 노력(ex. 소모된 PC 전력 및 전기의 양)에 대해 무료 코인으로 보상을 받습니다.

간단히 상상해 보세요, 5번 사람이 페이지의 봉인 번호를 알아낸다면, 그는 약간의 무료 코인, 예를 들어 1달러를 받게 되는데, 그것은 공기 중에서 만들어지는 것입니다. 바꿔 말하면, 5번 사람의 계좌 잔액은 다른 누군가의 계좌 잔액을 감소시키지 않고 1달러씩 증가합니다.

이것이 바로 비트코인이 존재하게 된 방법입니다. 5번이 받은 1달러는 블록체인(즉, 거래 내역을 나눠서 기록하는 네트워크)에서 거래된 첫번째 화폐입니다. 네트워크에서 각종 노력을 지속하고, 사람들은 비트 코인을 받습니다.

충분히 많은 사람들이 비트코인을 소유하면, 비트코인의 가치가 증가하여, 더 많은 사람들이 비트코인을 원하게 되고, 그것이 반복될 수록 가치는 커지게 됩니다. 이러한 보상은 모든 사람들이 네트워크에서 계속 일하게 만듭니다.

그리고 모든 사람들이 그들의 폴더 안에 있는 페이지를 없애고 나면, 그들은 새로운 빈 페이지를 꺼내서 위의 과정을 다시 반복하게 되는데, 그 과정은 영원히 반복됩니다.

여러분, 이것이 바로 블록체인이 구동되는 방식입니다.

아, 아직 한가지 얘기하지 않은 것이 있습니다.

폴더에 이미 봉인 번호로 봉인된 5장의 페이지가 있다고 가정해 봅시다. 본인을 위해 2번째 페이지로 돌아가서 거래 내역을 수정하게 된다면 어떻게 될까요? 봉인 번호는 네트워크의 모두가 거래 내역이 불일치하는 것을 확인할 수 있게끔 해줍니다. 만약 수정된 거래 내역에 새로운 봉인 번호를 계산하고 대신 페이지에 별도의 라벨을 지정해 버리면 어떠한 상황이 생길까요?

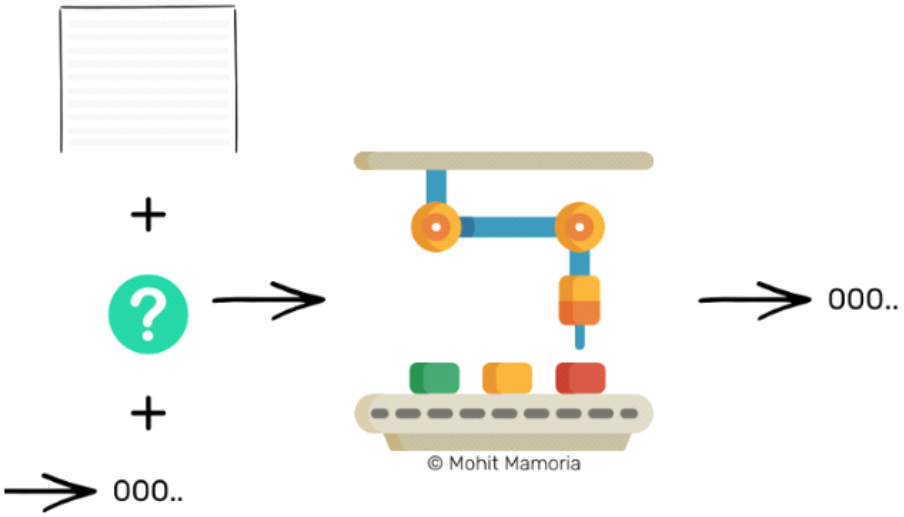
누군가 과거의 특정 페이지로 돌아가서 페이지(Block) 및 봉인 번호를 수정하는 것을 미연에 방지하기 위해, 봉인 번호를 계산하는 방법을 약간 뒤틀어볼 필요가 있습니다.

봉인 번호를 무단 수정하는 것에 대한 방지 대책

제가 앞에서, 여러분에게 20893이 적힌 상자 외에도 계산을 위한 빈 상자 하나를 여러분에게 더 주었다는 것을 기억해 보세요. 실제로, 블록체인의 봉인 번호를 계산하기 위해서 두 개의 상자 대신에 미리 채워진 두 개의 상자와 이미 계산된 한 개의 상자, 총 3개의 상자가 준비되어 있습니다.

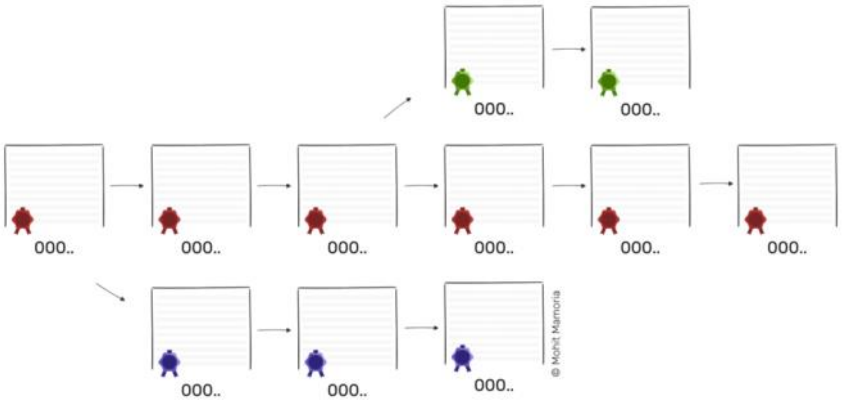
왼쪽에서 기계에 3개의 채워진 상자가 밀어넣어질 때, 오른쪽에서 나오는 결과값은 반드시 필요한 어떤 조건을 충족시켜야만 합니다.

우리는 이미, 하나의 상자에 거래 내역이 존재하고 있고 하나의 상자에는 봉인 번호가 포함되어 있는 것을 알고 있습니다. 마지막 세 번째 상자에는 이전 페이지에 대한 마법 기계의 출력이 들어가 있습니다.



이러한 작은 방법으로, 모든 페이지는 이전에 작성된 페이지에 의존한다는 것을 알아낼 수 있습니다. 따라서, 누군가가 이전 페이지를 수정해야 한다면, 그 일관성을 유지하기 위해 모든 페이지의 내용과 봉인 번호까지 변경해야 할 것입니다.

위의 이야기들에서 나온 10명 중 한명이 블록체인(거래 내역이 적힌 페이지가 들어있는 폴더)의 내용을 속이고 무단으로 수정하려면, 모든 페이지의 내용을 바꾸고 봉인 번호까지 새로 계산해야 합니다. 우리는 봉인 번호를 계산해 내는 것이 얼마나 어려운지 알 수 있습니다. 그러므로, 네트워크 내 한명의 부정직한 사람은 아홉명의 정직한 사람을 이길 수 없습니다.



정직하지 못한 사람이 속이려고 하는 그 페이지에서 네트워크 상에 또 다른 체인을 만드는 일이 일어날 수도 있지만, 그 체인은 결코 그 정직한 체인을 넘어설 수 없습니다. 단지, 한 사람의 노력과 속도는 그 동안 누적된 노력과 속도를 넘어설 수 없기 때문이다. 그러므로 **네트워크에서 가장 오래 이어져 온 긴 체인이 가장 정직한 체인임을 보장받을 수 있습니다.**

정직하지 못한 한 사람이 아홉명의 정직한 사람들을 이길 수 없다는 사실을 들었을 때, 여러분의 머릿속에 어떠한 다른 생각이 떠오르지 않나요?

한 명이 아니라, 여섯 명이 정직하지 못한 사람들이라면?

이러한 경우에, 해당 프로토콜은 실패한 것이나 마찬가지입니다. 이것은 흔히 비트코인계에 알려진 “51% 공격”입니다. 네트워크 안에 있는 대다수의 개인들이 정직하지 않게 변하여 나머지 소수를 속이기로 결정한다면, 그 체인은 목적을 잃게 될 것입니다.

그리고 **이것은 블록체인이 붕괴될 수 있는 유일한 취약점입니다.** 그것이 일어나기 어렵다는 것을 알지만, 시스템의 취약한 부분들을 모두 알아야 합니다. **블록체인은 군중의 대다수가 항상 정직하다는 가정 하에 만들어진 것**입니다.

출처 : http://media.fastcampus.co.kr/knowledge/wtf_blockchain_bitcoin/