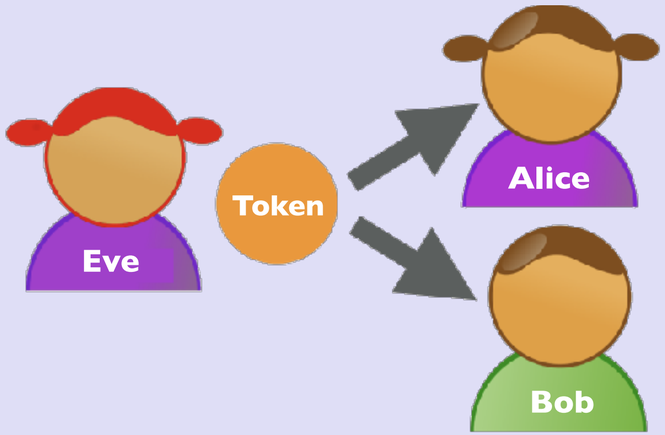
BLOCKCHAIN TUTORIAL 22

Double spending, third party



ECASH

- In 1983 ecash was conceived by David Chaum as an anonymous cryptographic electronic money.

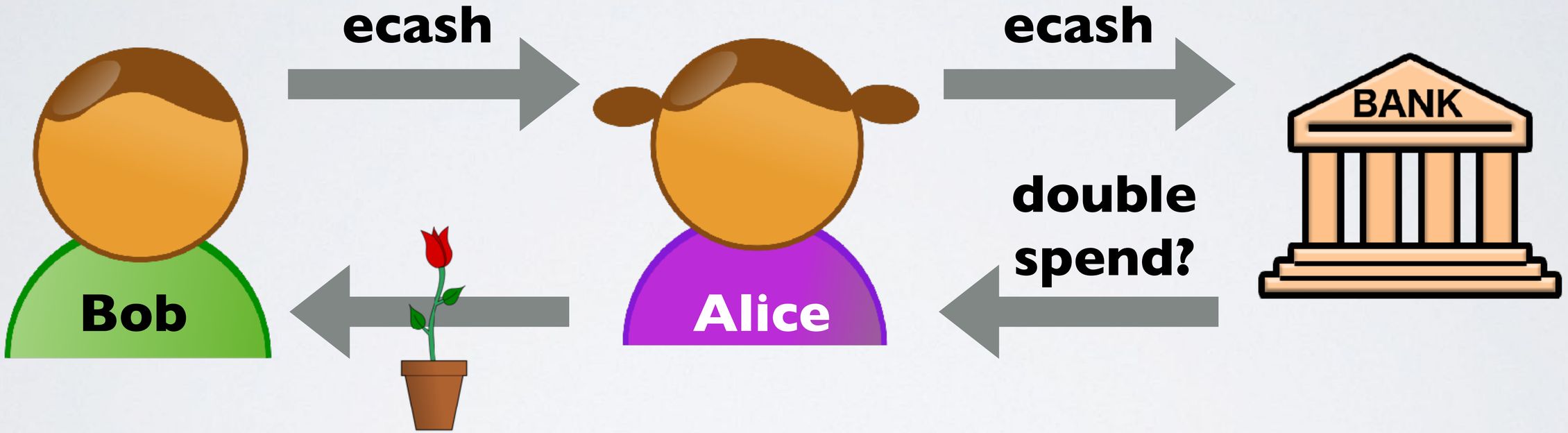
- It worked as follows, this is a simplified explanation: A Bank created the electronic money which are cryptographically signed. The digital money contained an unique id also known as token. Users can purchase these digital money.

- Bob wants to buy things from Alice's shop, he sends her the required ecash value. Having received the payment she sends the ecash to the issued Bank and waits for acceptance. The Bank checks if the ecash token has not already been spend. Alice sends the goods after the Bank has informed her that the ecash is valid.

- In 1998 the use of ecash was abandoned mainly because credit cards was the consumers choice for payment.

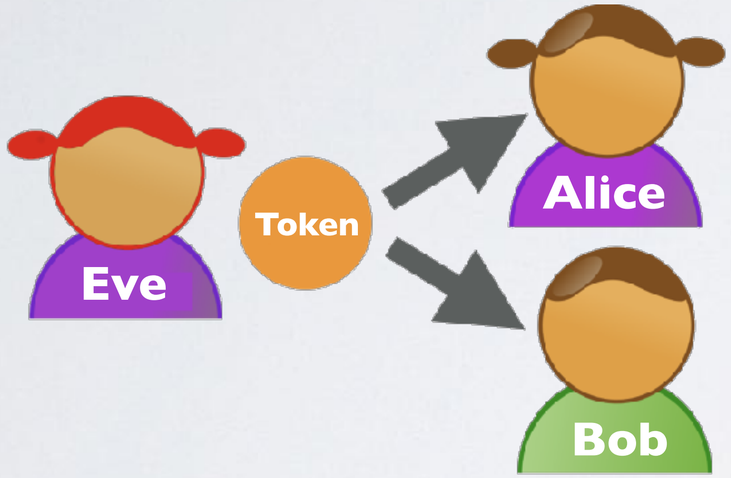
DOUBLE SPENDING

- The ecash system needed a third party (Bank) to check if the digital money is not double spend because electronic files can be easily duplicated.



THIRD PARTY

- The double spending problem is the main problem you need to solve if you introduce a new electronic money scheme.



- This problem can be solved by using a online central trusted third party that can verify whether a token has been already spent.

- This third party can be a bank, broker or any entity which facilitates interactions between two parties who both trust the third party.

DISADVANTAGES USING THIRD PARTIES

- Here are a few disadvantages using third parties related to financial services:

  - The 2008 financial crisis were several banks failed teaches us that there is no such thing as a trusted third party. They fail because of mismanagement, greed or they can be involved in illegal bank activities.

  - Half of the adults around the world doesn't have access to financial services because the financial institutions are too far away and/or too expensive to use. Third parties are commercial entities and they will charge fees for their services. If you invent a new electronic money one of the goal is to make it accessible and payable to anyone in the world.

DISADVANTAGES USING THIRD PARTIES

- Third parties have the power to suspend customers accounts. For example, in 2010 PayPal has suspended WikiLeaks donation account and froze its assets. PayPal claims WikiLeaks to encourage others to engage in illegal activity. This was not a result of a legal process but rather, are a result of fear of falling out of favour with Washington.

- Third parties can deny or limit access to your assets. For example, in 2015 Greek banks limited cash withdrawals because of the rush on the banks. The Greeks grew fearful of the possibility of an economic collapse.

SOLVING DOUBLE SPENDING WITHOUT THIRD PARTY

- Bitcoin was the first application which has solved the double spending problem without the use of a central trusted third party.

- Satoshi Nakamoto conceived Bitcoin and created its original reference implementation.

- Satoshi Nakamoto solved the double spending problem using a technology what is now called today the Blockchain technology. The system is based on cryptographic proof instead of trust.

- Blockchain technology was originally used as a cryptocurrency for payment transaction between two parties but nowadays it can be used for example in notary services, identity services, voting, etc.