



Курсовая работа: Реализация в FPGA прототипа майнера для BitCoin

Выполнила студентка 208 группы

Е. Д. Глазова

Научный руководитель:

к.ф.-м.н. Г. А. Лукьянченко

How a blockchain works

1

A wants to send money to B



2

The transaction is represented online as a 'block'



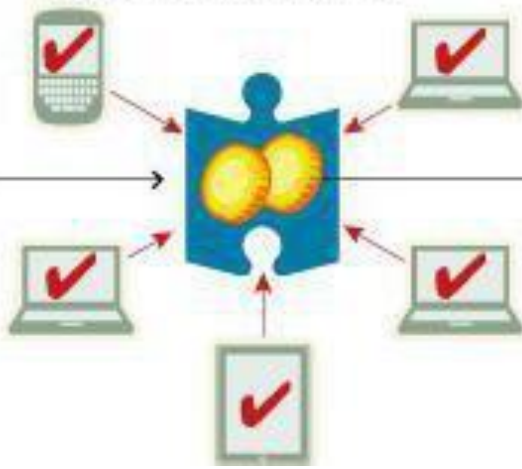
3

The block is broadcast to every party in the network



4

Those in the network approve the transaction is valid



5

The block then can be added to the chain, which provides an indelible and transparent record of transactions



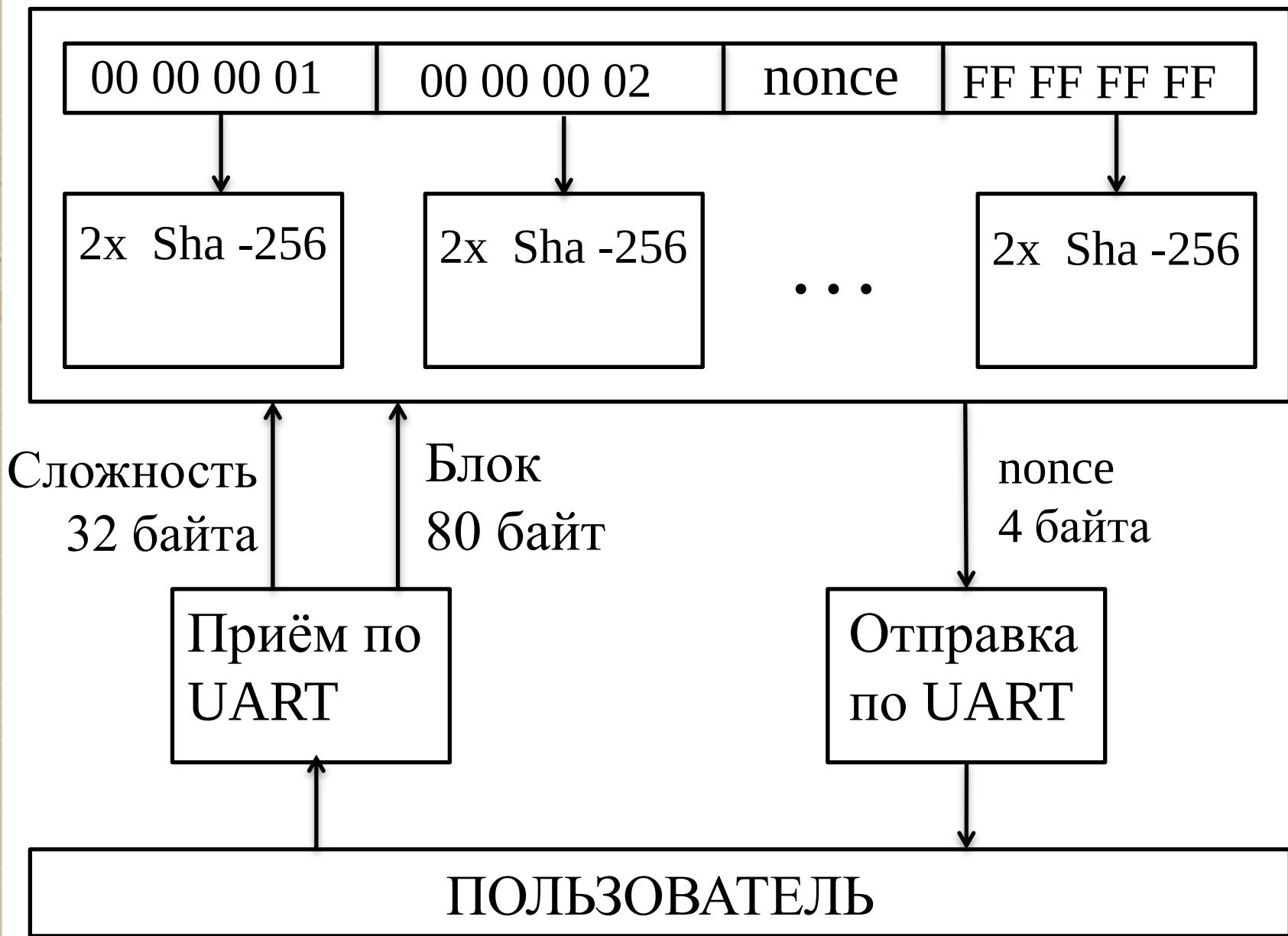
6

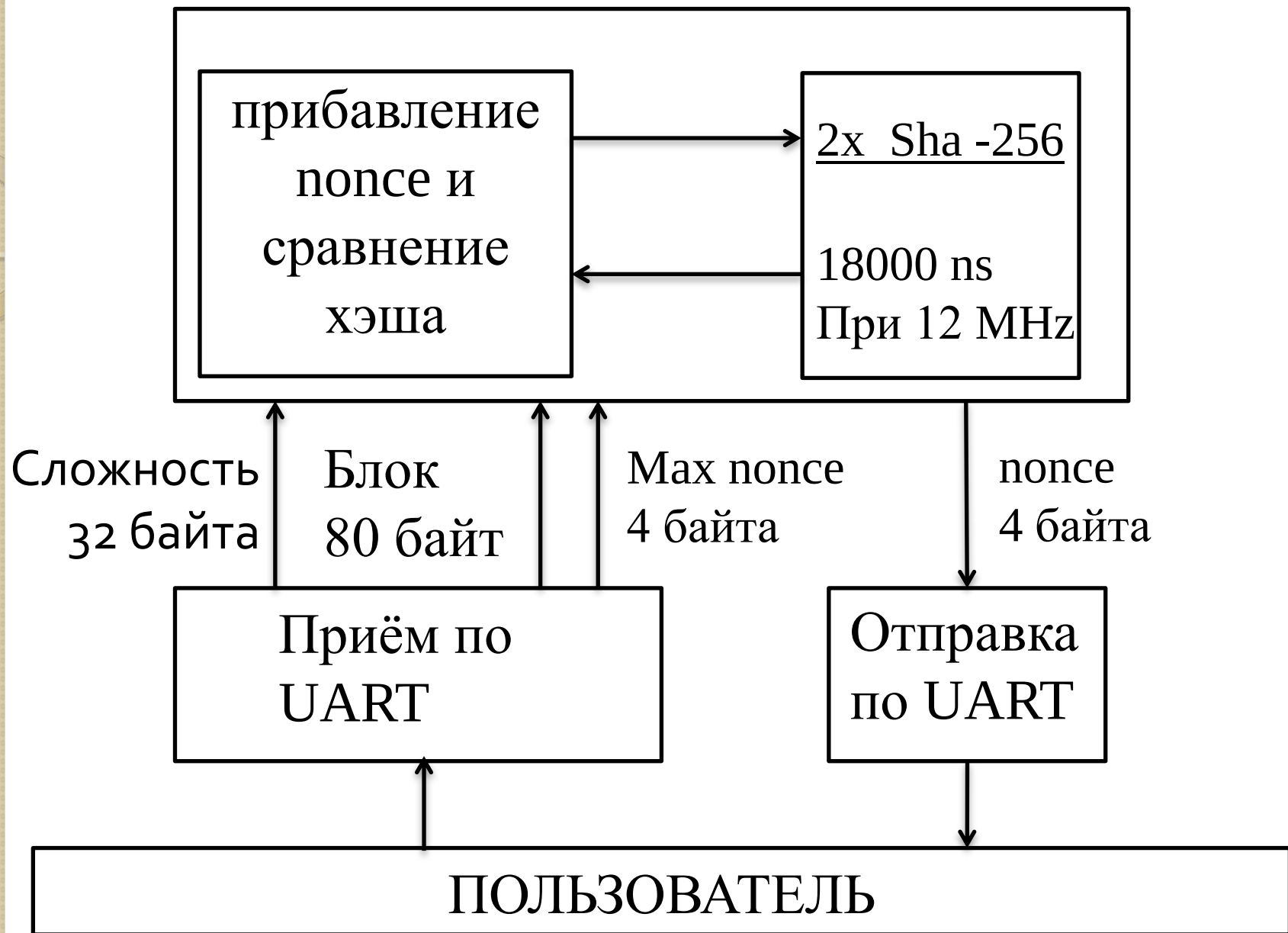
The money moves from A to B



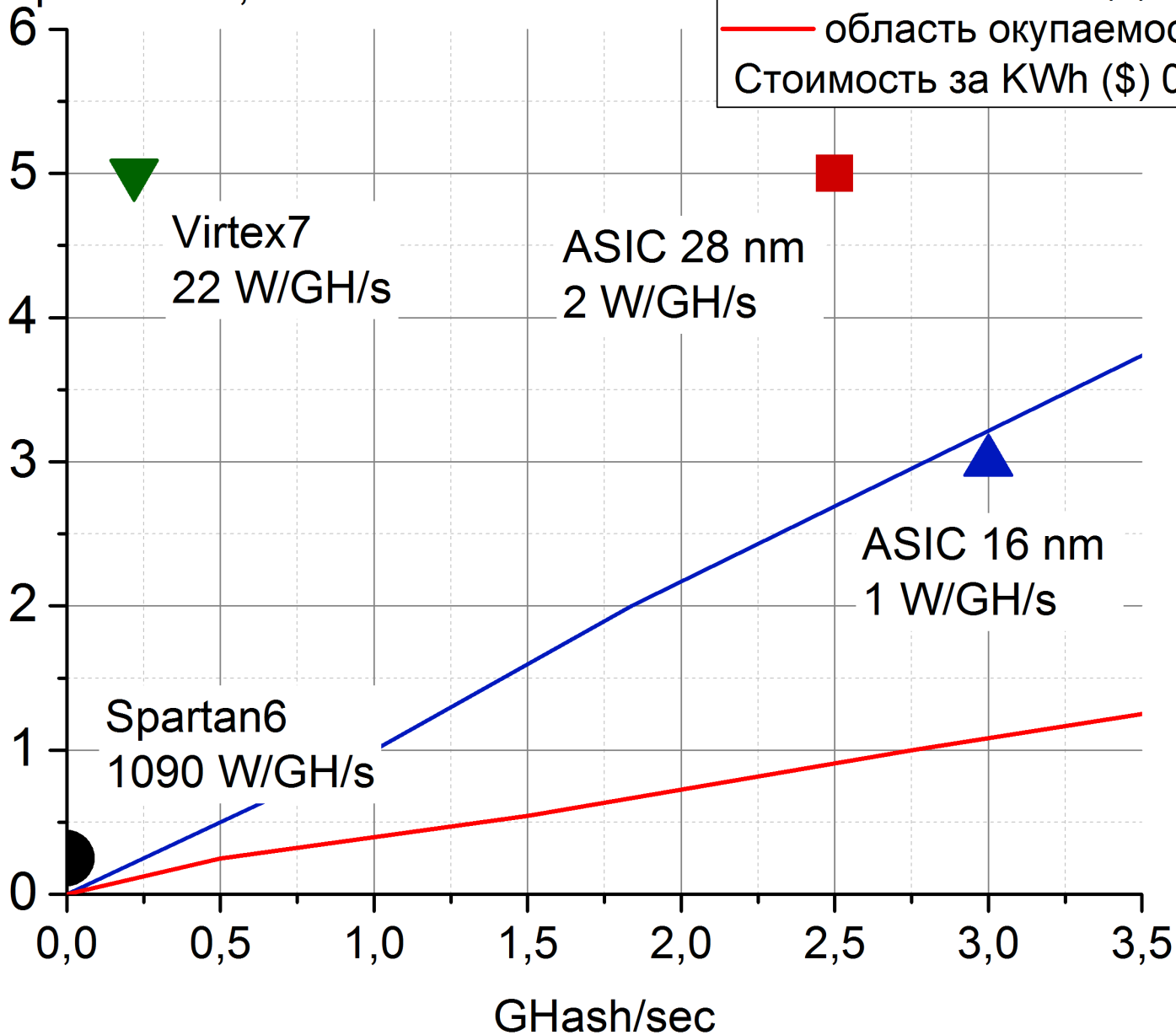
BitCoin блок для хэширования

Поле	Назначение	Обновляется когда...	Размер (Байт)
Version	Номер версии блока	Происходит обновление программного обеспечения (указывает новую версию)	4
hashprevblblock	256-битный хэш заголовка предыдущего блока	Изменяется предыдущий блок	32
hashMerkleRoot	256-битный хэш на основе всех транзакций в блоке	Добавляется новая транзакция	32
Time	Текущая отметка времени в секундах с 1970-01-01 00: 00 UTC	Каждые несколько секунд	4
Bits	Текущая сложность (256 битное число) в компактном формате	Изменяется сложность	4
Nonce	32-разрядное число	Хэш не удовлетворяет сложности (на каждой итерации)	4



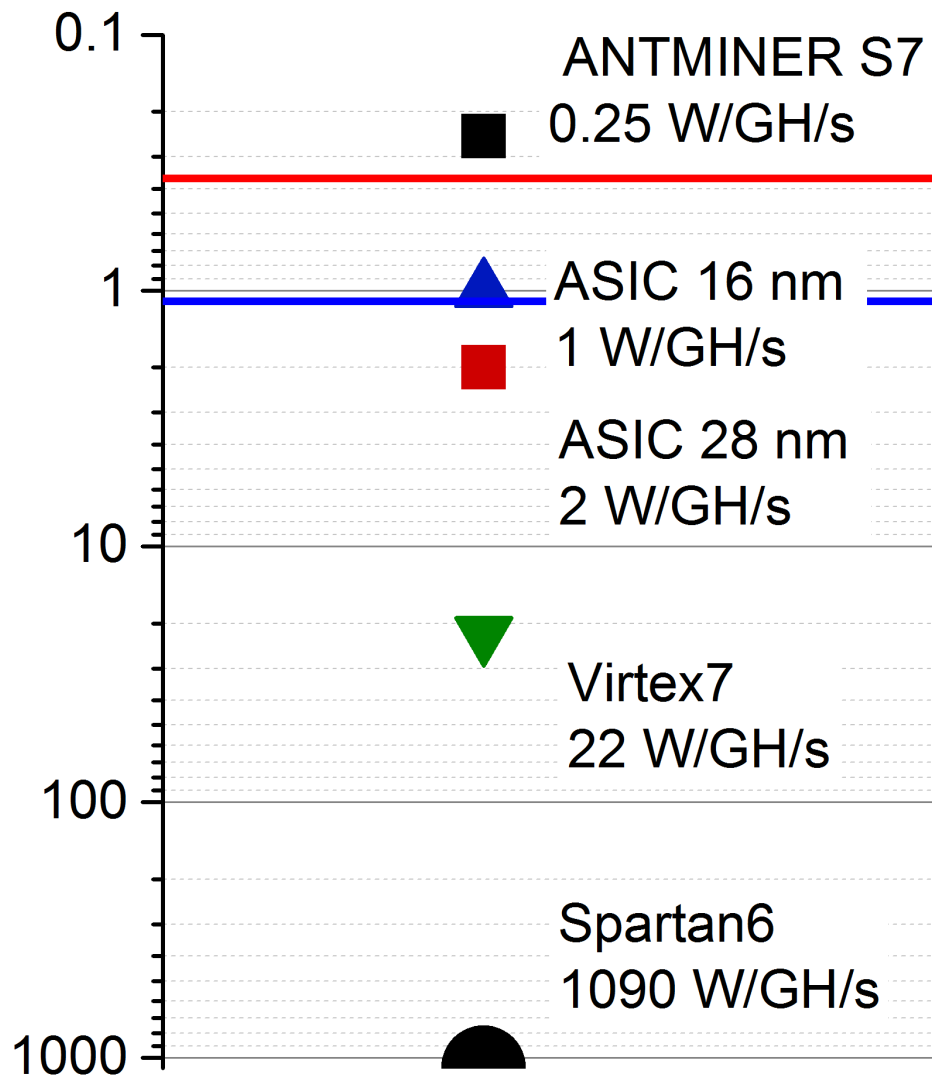


Энергопотребление, W



— область окупаемости ночью
Стоимость за KWh (\$) 0.02
— область окупаемости днём
Стоимость за KWh (\$) 0.06

Энергоэффективность, W/GH/s



область окупаемости
ночью

Стоимость за KWh (\$) 0.02

область окупаемости
днём

Стоимость за KWh (\$) 0.06

Результаты

- Изучена система работы BitCoin принципы майнинга
- Реализован в ПЛИС прототип полноценного масштабируемого майнера BitCoin
- Произведены оценки энергоэффективности полученного дизайна



Спасибо за внимание!