AlphaWallet

AlphaWallet Blockchain Ticket Test Report

2018 Russia World Cup ERC875 Tickets

AlphaWallet

August 2018

AUTHOR

AlphaWallet Zhongnan Zhang

Co-founder and CEO of AlphaWallet (Stormbird Pte. Ltd.). Chinese Australian resident. With more than 10 years of experience in the ticket market, he has managed multinational teams and companies in Asia Pacific countries (China, Australia, Singapore, Japan, Korea, Malaysia) for more than 7 years. He helped 360Experience (one of Ticketbis's three business units) enter the Asia Pacific market successfully, and was acquired by eBay in 2016 for $165 million. He is a continuous entrepreneur and has established five companies in Australia, Beijing, Hong Kong and Singapore. He is a technology enthusiast who started to work with the blockchain in 2014 and tried to use the blockchain technology to reconstruct the popular event ticket market and holds a small amount of Bitcoin and Ethereum. He is also a Wing Chun and boxing lover.

SHANKAi 盛开体育 郑来

Vice President of Blooming Sports. He is head of the 19th, 20th, and 21st World Cup official ticketing in China. He used to be responsible for the Citizens' outbound business of China Travel Service Group and has worked for CITIC Group International Financial Holdings Group Co., Ltd. in charge of investment in the tourism, aviation and sports sectors.

SHANKAi 盛开体育 高东东

IT Manager of Shankai Sports。He has been responsible for the operation of ticket management for many international event (2014-2018 World Cup, 2016 European Cup, Champions League, Barcelona Club, etc.). He started to work with the blockchain in 2016 and has been working closely with AlphaWallet (Stormbird Pte. Ltd.) since 2017. They apply new Internet technologies to international top-level event tickets, and has been working to open the Chinese market for international events through ticketing channels and promote the rapid development of China's sports industry.

CONTENTS

INTRODUCTION

ALPHAWALLET

AlphaWallet (Stormbird Pte. Ltd.) is a blockchain startup focused on Layer 2, Offchain blockchain protocol development and consumer terminal application platform development to Improve the usability, performance and privacy of blockchain. The AlphaWallet App is an Ethereum smart contract tool and a protocol runtime platform for the average consumer. ERC 875 is a non-fungible token standard for business cases. Developers and businesses can easily use ERC 875 token to refer to People, Things, Objects and Rights in the physical or digital world, and achieve efficient atomic transaction.

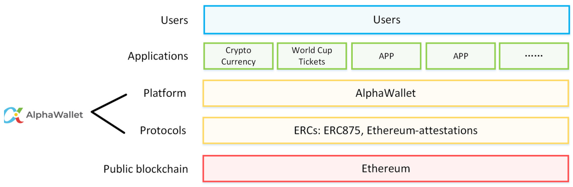


Fig 1. AlphaWallet Platform

SHANKAI SPORTS

Beijing Shankai International Travel Agency Co., Ltd. is a fast-growing sports marketing company that provides sports business operations solutions for domestic and foreign investors. They have a deep understanding of the local market and have a special domestic and international network. They have extensive experience in major international sports events and fully understand the needs of international sports event participants. Making full use of sports as an advertising platform to help Chinese brands continue to grow, they will introduce the world's top events to China and use digital media technology to enable Chinese sports enthusiasts to get close to the action.

PRIMARY MARKET

The primary market refers to the market consisting of officially authorized channels under the supervision of the event organizer, such as the organizer's own official sales website, Damai.com, Yongle Ticket and other officially authorized ticketing platforms and sales organizations.

SECONDARY MARKET

The secondary market refers to the market consisting of sales channels that are not officially authorized by the organizer, including individuals, professional ticket sellers, and P2P market platforms.

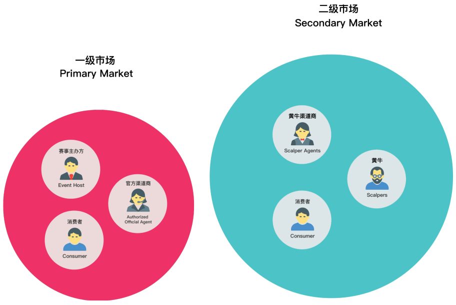


Fig 2. Primary market and secondary market

BLOCKCHAIN TECHNOLOGY

The blockchain is a distributed ledger technology that ensures information represented in each record is not easily falsified, therefore blockchain makes it easy to verity the ownership of each things represented on the ledger. At the same time, because the public chain is a public ledger, there is no barrier to entry, so ownership can be freely circulated and transferred directly. With the rise of Ethereum, in addition to recording, it can also support smart contracts to achieve various circulation logic.

At present, blockchain technology is still at a very early stage. In addition to experimental projects, there are only a few real-world scenarios that are suitable for commercialization. The data currently suitable for putting on the blockchain needs to meet the following principles:

1. **The information represented by the data has high value.** Such as money, important Rights, etc.

2. **The information presented by the data needs to be proven when using it (or reflecting its' value).** For example, when use Alipay, you need your Alipay account, Bank or a Clearing System to provide your funds flow.

3. **The ownership of things represented by the information can be circulated, transferred and altered**. Such as various exchange vouchers, etc.

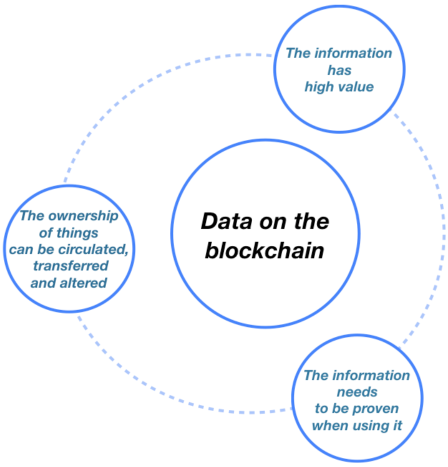

The information has high value
Data on the blockchain
The ownership of things can be circulated, transferred and altered
The information needs to be proven when using it

Fig.3 The principles that blockchain needs to meet

At this stage, if the data cannot satisfy the above three points at the same time, there are other technologies that are much better than the blockchain to meet the corresponding requirements. The most typical counterexample is identity information, which conforms to 1 and 2, but there is basically no use case for transferring ownership. The existing mature Attestation technology can better meet the usage requirements. There are also various kinds of deposit-type applications, etc. The blockchain is a ledger that is not a database, and is not used to store "evidence" when various ownership does not need to be transferred.

ISSUES WITH THE TICKET MARKET AND BLOCKCHAIN SOLUTIONS

01/ SECONDARY MARKET AND TICKET FRAUD

Both buyers and sellers have a love-hate relationship with the secondary market. For most popular events, the secondary market is much larger than the primary market, regardless of the price or amount of tickets available.

Affected party	Problems
Organizer	It is difficult to get the deserved benefits from the secondary market It is hart to obtain market data hard and still have to pay high fees Negative information in the secondary market affects the organizer's brand and reputation
Consumer	There is no supervision in the secondary market （There are a large number of scalper tickets and fake tickets） Consumer interests cannot be guaranteed
Officially Authorized Sales Channel	Scalper touting tickets has a negative impact on the official authorized sales channels.
Secondary Market Sales Channel	Lack of official authorization, and lack of trust Long payback periods Pay a high commission to the market that provides guarantees （The guarantee market needs to bear huge risks）

Table 1 Current problems in the ticket market

Current ticket market issues

For the organizer

It's good that the secondary market has increased the reach of events and activities around the world. But at the same time, because the secondary market is completely unregulated by the organizers, they have no way to get the benefits they deserve from the secondary market. They don't receive any money, so there is no way to prove to sponsors how big the scale of the secondary market is. The primary market is often monopolized by large channel dealers who have large fees that the organizer often cannot pay. In addition, there are a lot of negative aspects about the secondary market, such as fake tickets, high prices, etc., that affect the sponsor's brand and reputation.

For consumers

The existence of the secondary market is great for some consumers. At the same time, because it’s completely unregulated, there’s no way to protect consumers from the many High-priced and fake tickets floating around the secondary markets. And then sometimes hoarding behaviors still prevent people from buying a ticket even when there is still an empty seat in the venue.

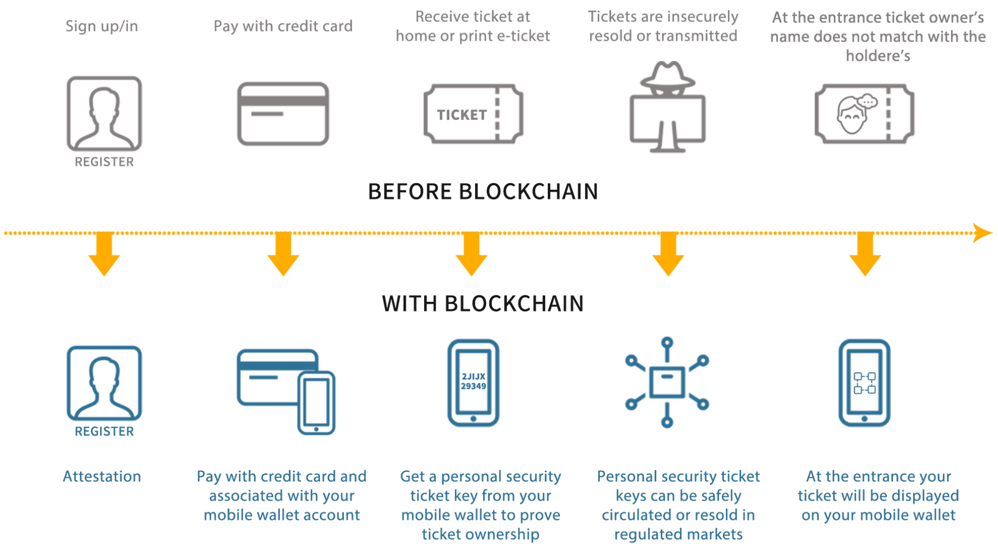
For officially authorized sales channels

The secondary market is usually a necessary channel for them to handle inventory. However for popular activities, scalpers snap up and hoard a large amount of tickets to make money reselling, which has a very bad impact on the reputation and profit of officially authorized sales channels.

For secondary market sales channels

The secondary market sales channel has injected more liquidity into the entire ticket market, while providing consumers with greater convenience. However, sellers in the secondary market do not have an official endorsement, so they pay high fees to guaranteed markets such as Viagogo, Stubhub, Taobao, etc. to gain consumers’ trust. And thus , these markets that provide guarantees also bears a huge amount of risk.

Blockchain Solutions



Sign up/in
Pay with credit card
Receive ticket at home or print e-ticket
Tickets are insecurely resold or transmitted
At the entrance ticket owner’s name does not match with the holdere’s
REGISTER
TICKET
BEFORE BLOCKCHAIN
WITH BLOCKCHAIN
REGISTER
2JIJX 29349
Attestation
Pay with credit card and associated with your mobile wallet account
Get a personal security ticket key from your mobile wallet to prove ticket ownership
Personal security ticket keys can be safely circulated or resold in regulated markets
At the entrance your ticket will be displayed on your mobile wallet

Fig.4 Convenience that blockchain brings to consumers

For the organizer

- Various rules can be defined using smart contracts to achieve regulation of the primary and secondary markets. For example, an organizer can create rules for ticket A that 1) it's only allowed to resell 5 times; 2) the resale price cannot exceed 100; 3) the maximum profit for each resale shall not exceed 10%; If the profit is less than 5%, FIFA will not charge a profit commission; if it exceeds 5%, FIFA will charge 50% profit commission.
- The specific figures of the secondary market scale can be directly collected, and the entire process of ticket circulation can be monitored and controlled.
- Can directly profit from each secondary market transaction. The commission will automatically return to the organizer in the prescribed proportion.
- Can connect to each ticket holder directly and know the wallet address of each user.

For consumers

The supervised secondary market will be healthier, increasing usage and liquidity.

- Lower ticket prices
- No more fake tickets
- Buy tickets at any time
- Enjoy the convenience of digitalization;
- And more. Such as Enjoy discounts in specific shopping malls when you hold the blockchain ticket as a certificate.

For officially licensed market platforms

- Secondary sales platform aren't able to monopolize data and capital flows. The organizer owns the information and controls it based on consumer permissions. Through atomic transaction, the funds flow goes into the organizer or other ticket seller account directly, and no longer passes through the sales platform market.
- The function of the sales platform market is simplified to marketing and transacting, without settlement or data analysis.

For official ticketing agencies

- More sales channels options because any organization can join the open blockchain market and start selling ticket.
- Reduced how much revenue relies on user data.
- Reduced how much revenue relies on billing.

For the secondary market platform

- Similar to the officially licensed market, the secondary market platform has no chance to monopolize data or capital flows.
- The atomic transaction replaces the guarantee function of the secondary market platform and forces secondary market platforms to significantly reduce their fee percentage (At this stage, 15% - 30% of the total amount for each transaction is for the platform Service fee).

For ticketing institutions in the secondary market

- No longer need an intermediary platform to provide guarantees, thus significantly increasing the number of customers reached expanding sales, and reducing costs.
- Through this atomic transaction, fees can be collected in time.
- No longer possible to earn a super high profit, because now subject to supervision by the official ticket agency.
- Small profits but quick turnover.

02/ PAYMENT FRAUD

Payment fraud is a big problem for all companies. Every year there are a large number of credit card thefts, charge disputes, fake cards, etc. That caused huge losses for businesses. For the event ticket industry, this requires two parts to support: blockchain tickets plus blockchain currency (cryptocurrency). Atomic transactions can be achieved and payment fraud can be completely eliminated only when the two are used at the same time.

03/ ACTIVITY SAFETY KYC (KNOW YOUR CUSTOMER)

This part is not a direct benefit of blockchain tickets. However, digital tickets bring benefits on there own, and blockchain is the best solution for digital tickets.

Attestation is mainly used here. The best place to put this technology is on the client side (encrypted wallet). The client can generate Attestation or import Attestation provided by the third-party certification authority (such as the mobile number verification, ID card or passport that provided by the government, etc.), and the smart contract and the website have built-in method for verifying Attestation. Smart contracts and websites give different feedback when different users submit different Attestations.

The final implementation is similar to:

- Anyone who is not on the blacklist can hold ticket A
- Only Chinese users can hold tickets B
- Only users born before 1958 can hold tickets C
- Only user XXX can hold ticket D
- Only the user XXX can hold the ticket D. User's biometrics are required for authentication when entering the event venue, such as fingerprints.

Various levels of KYC can be achieved by binding several kinds of user information. The safety of the event can be greatly improved through strict KYC.

04/ FREE CIRCULATION UNDER SUPERVISION

Smart contracts are developed and Tokens are issued on the public chain：

- The public chain helps tokens to confirm the authorization, and allows tokens to achieve free circulation without permission.
- Smart contracts can customize the circulation and usage rules for each token in advance.

Combining the two points, the token can be freely circulated under supervision.

In a smart contract, a token can represent various Things, Objects and Rights in digital world or physical world. For a better understanding, we divide tokens into two categories artificially:

- **PHYSICS TOKEN - Token represents the Things, Objects and Rights in the physical world**
- **DIGITAL TOKEN - Token represents the Things, Objects and Rights in the digital world**

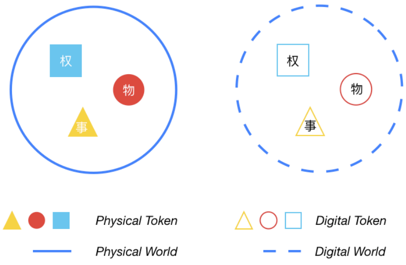
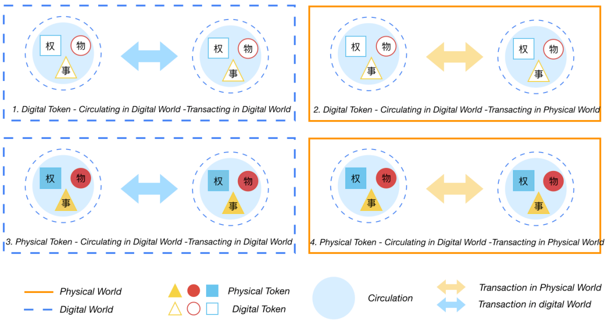


Fig.5 Physics token and digital token

Four ways of Token Circulation and Usage

1. Digital Token - Circulating in Digital World - Transacting in Digital World
2. Digital Token - Circulating in Digital World - Transacting in Physical World
3. Physical Token - Circulating in Digital World - Transacting in Digital World
4. Physical Token - Circulating in Digital World - Transacting in Physical World



权
物
事
1. Digital Token - Circulating in Digital World -Transacting in Digital World
2. Digital Token - Circulating in Digital World -Transacting in Physical World
3. Physical Token - Circulating in Digital World -Transacting in Digital World
4. Physical Token - Circulating in Digital World -Transacting in Physical World
Physical World
Digital World
Physical Token
Digital Token
Circulation
Transaction in Physical World
Transaction in digital World

Fig.6 Tokens Circulation and Usage

Physics Token - Circulating in Digital World - Transacting in Physical World

The first way is very common. Such as various types of consumption tokens (ETH, etc.) in the public chain.Digital Token is used for transaction. For example, digital assets transaction.

Digital Token - Circulating in Digital World - Transacting in Physical World

It is the most popular way. Including various public chains which purpose is to replace currency, such as BTC, and using tokens to buy Things, Objects and Rights in the physical world.

Physical Token - Circulating in Digital World - Transacting in Digital World

It is rare to use because the Things, Objects and Rights in the physical world are not easily used in the digital world. This type of token is rare at present.

Physical Token - Circulating in Digital World - Transacting in Physical World

Most of the real-world applications, such as blockchain tickets, are used the fourth way.

Central Trust Agency: Gateway

The Central Trust Agency is the bridge between token and the physical world. It is a gateway that tokenizes the Things, Objects and Rights in the physical world. The gateway can also transform tokens to the Things, Objects and Rights in the physical world. The central Trust Agency must have sufficient credit degree to support the Things, Objects and Rights represented by the tokens and then implement the gateway function.

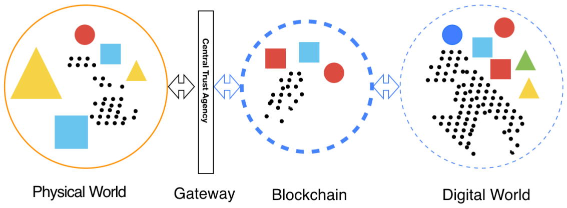


Fig.7 Central trust agency: Gateway

For examples:

- A dumpling restaurant can issue Dumpling Token to represent dumpling; It has enough credit to make people believe that this Token can be used to exchange for a dumpling.
- The Housing Management Office can issue a Token to present the ownership of a house.Its' credit makes people believe they own this token means they have the ownership of this house.
- The landlord and the housing agency use a Token to represent the right to use a house for one to three months. They have good credit to make people believe If they have the toke, they would have the right to use the house for one to three months
- The government can issue a Token to replace currency. Government's credit can convince everyone that "owning and using" the Token is the same as "owning and using" existing currency.

The Things, Objects and Rights in the physical world are tokenized in the public chain, which increases the property of its free circulation. Blockchain confirmation leads to circulation property. A public shared ledger replaces the third-party agency to confirm. It brings some benefits. Any distribution channel can freely join the circulation of the token and no need to sign a contract with a third party, and get through the database any longer. Meanwhile, the Central Trust Agency can set various rules in the smart contract for issuing tokens to realize the free circulation of each token's own rules on the public chain, thus achieving free circulation under supervision.

THE TEST RESULT OF 2018 RUSSIA WORLD CUP ERC 875 TICKETS

SOLUTIONS

Solutions for the 2018 Russia World Cup ERC 875 Ticket	
Public Chain	Ethereum
Contract Standard	ERC 875 NFT
Contract Address	0xA66A3F08068174e8F005112A8b2c7A507a822335
Contract Source Code	Based on ERC 875 https://github.com/alpha-wallet/contracts/blob/master/FIFA%20WC2018/schema1/TicketingContract.sol
Organizer APP	Usher Mobile App (Code is about to open source.) Reference https://github.com/alpha-wallet
User APP	AlphaWallet (Code is about to open source.) Reference https://github.com/alpha-wallet
Data Management	Akio’s Solution

Table 2 solutions for the 2018 Russia World Cup ERC 875 Ticket

PUBLIC CHAIN：ETHEREUM

Reasons for choosing Ethereum are as follows:

1. World Cup tickets have high liquidity, so the most widely accepted public chain, that is Ethrerum, is needed.
2. The blockchain ticket test does not allow any error, because of the importance of the World Cup. Ethereum is the most mature and stable one in the public chain to support smart contracts.
3. The price of World Cup tickets is high. Relatively speaking, the cost of gas in Ethereum is not significant.
4. World Cup tickets are sold in advance, and it is rarely traded at the last minute before the event started, even in the secondary market. So the performance of Ethereum meets the trading needs.

SMART CONTRACT STANDARD：

ERC875 NFT（NON-FUNGIBLE TOKEN）

After comparing the two NFT standards ERC721 and ERC875, We finally chose ERC875. Reasons are as follows：

1. ERC875 makes it easier to implement atomic transaction. AlphaWallet developed MagicLink based on ERC 875 [1]：

   a) The organizer sends a MagicLink to users by several ways. Users can directly import one or more World Cup tickets by the MagicLink without Ethereum.

   b) Users can create a MagicLink in AlphaWallet to export their own tickets. First send the MagicLinc to the receiver; then the receiver clicks the link and import the ticket; the gas paid by Shankai Sports. Both the sender and the receiver do not need to pay the gas when transferring is free.

   c) Sellers use AlphaWallet to create MagicLinks, send them to buyers or publish it in markets to sell their tickets. Buyers click the MagicLink, check the ticket information and price on the AlphaWallet, and confirm. When the buyer pays the fare and receives the ticket, the seller receives the money and ticket disappears. An atomic transaction is completed.

2. ERC875 can transfer multiple NFTs at once: In the ticketing scenario, it is usually necessary to transfer multiple tickets at the same time, as few as 2 and as many as 20,000. ERC875 allows us to transfer any number of tickets at once.

SMART CONTRACT ADDRESS：

0xA66A3F08068174e8F005112A8b2c7A507a822335

[1] MagicLink Demo
https://app.awallet.io/AJiWgGD8wLWmaj8IBoF06PAFESqLLHpQeoljNRgS98-1lbStj40j8DWNqUbfDl91bgh9gQako6Ngq1K6SgTHAzyL0cByPkLdu1a-YSIQJngSjveAvW9nXkwN24MFGw==

SMART CONTRACT SOURCE CODE：

BASED ON ERC 875

https://github.com/alpha-wallet/contracts/blob/master/FIFA%20WC2018/schema1/TicketingContract.sol

```
//mainnet: 0xA66A3F08068174e8F005112A8b2c7A507a822335

// ["0x474d542b330000000000000000000000020b5b23d4704d415249524e04050001",
// "0x474d542b330000000000000000000000020b5b23d4704d415249524e04050002",
// "0x474d542b330000000000000000000000010a5b291a70504f4c53454e0f050001",
// "0x474d542b330000000000000000000000010a5b291a70504f4c53454e0f050002",
// "0x474d542b330000000000000000000000020b5b2944a052555345475911050001",
// "0x474d542b330000000000000000000000020b5b2944a052555345475911050002",
// "0x474d542b330000000000000000000000006055b3fae205735335735343a050001",
// "0x474d542b330000000000000000000000006055b3fae205735335735343a050002",
// "0x474d542b330000000000000000000000020b5b4a01e04c36314c36323f050001",
// "0x474d542b330000000000000000000000020b5b4a01e04c36314c36323f050002",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050001",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050002",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050003",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050004",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050005",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050006",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050007",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050008",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050009",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000a",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000b",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000c",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000d",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000e",
// "0x474d542b330000000000000000000000001075b2282f05255534b53410105000f",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050010",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050011",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050012",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050013",
// "0x474d542b330000000000000000000000001075b2282f05255534b534101050014"],
// "FIFA WC2018",
// "SHANKAI",
// "0x0D590124d2fAaBbbdFa5561ccBf778914a50BCca",
// "0xFE6d4bC2De2D0b0E6FE47f08A28Ed52F9d052A02",
// "0x2e558Bc42E2e37aB638daebA5CD1062e5b9923De"


pragma solidity ^0.4.17;
contract TicketPro
{
    mapping(address => bytes32[]) inventory;
    uint16 ticketIndex = 0; //to track mapping in tickets
    address organiser;
    address paymaster;
    uint numOfTransfers = 0;
    string public name;
    string public symbol;
    uint8 public constant decimals = 0; //no decimals as tickets cannot be split

    event Transfer(address indexed _to, uint16[] _indices);
    event TransferFrom(address indexed _from, address indexed _to, uint16[]
_indices);
    event Trade(address indexed seller, uint16[] ticketIndices, uint8 v, bytes32 r,
bytes32 s);
    event PassTo(uint16[] ticketIndices, uint8 v, bytes32 r, bytes32 s, address
indexed recipient);

    modifier organiserOnly()
    {
        if(msg.sender != organiser) revert();
        else _;
    }

    modifier payMasterOnly()
    {
        if(msg.sender != paymaster) revert();
        else _;
    }

    function() public { revert(); } //should not send any ether directly

    constructor (
        bytes32[] tickets,
        string nameOfContract,
        string symbolForContract,
        address organiserAddr,
        address paymasterAddr,
        address recipientAddr) public
    {
        name = nameOfContract;
        symbol = symbolForContract;
        organiser = organiserAddr;
        paymaster = paymasterAddr;
        inventory[recipientAddr] = tickets;
    }

    function getDecimals() public pure returns(uint)
    {
        return decimals;

    // example: 0, [3, 4], 27,
"0x9CAF1C785074F5948310CD1AA44CE2EFDA0AB19C308307610D7BA2C74604AE98",
"0x23D8D97AB44A2389043ECB3C1FB29C40EC702282DB6EE1D2B2204F8954E4B451"
    // price is encoded in the server and the msg.value is added to the message digest,
    // if the message digest is thus invalid then either the price or something else in the message is
invalid
    function trade(uint256 expiry,
                   uint16[] ticketIndices,
                   uint8 v,
                   bytes32 r,
                   bytes32 s) public payable
    {
        //checks expiry timestamp,
        //if fake timestamp is added then message verification will fail
        require(expiry > block.timestamp || expiry == 0);

        bytes32 message = encodeMessage(msg.value, expiry, ticketIndices);
        address seller = ecrecover(message, v, r, s);

        for(uint i = 0; i < ticketIndices.length; i++)
        { // transfer each individual tickets in the ask order
            uint16 index = ticketIndices[i];
            assert(inventory[seller][index] != bytes32(0)); // 0 means ticket gone.
            inventory[msg.sender].push(inventory[seller][index]);
            // 0 means ticket gone.
            delete inventory[seller][index];
        }
        seller.transfer(msg.value);

        emit Trade(seller, ticketIndices, v, r, s);
    }

    function loadNewTickets(bytes32[] tickets) public organiserOnly
    {
        for(uint i = 0; i < tickets.length; i++)
        {
            inventory[organiser].push(tickets[i]);
        }
    }

    function passTo(uint256 expiry,
                    uint16[] ticketIndices,
                    uint8 v,
                    bytes32 r,
                    bytes32 s,
                    address recipient) public payMasterOnly
    {
        require(expiry > block.timestamp || expiry == 0);
        bytes32 message = encodeMessage(0, expiry, ticketIndices);
        address giver = ecrecover(message, v, r, s);
        for(uint i = 0; i < ticketIndices.length; i++)
        {
            uint16 index = ticketIndices[i];
            //needs to use revert as all changes should be reversed
            //if the user doesn't't hold all the tickets
            assert(inventory[giver][index] != bytes32(0));
            bytes32 ticket = inventory[giver][index];
            inventory[recipient].push(ticket);
            delete inventory[giver][index];
        }

        emit PassTo(ticketIndices, v, r, s, recipient);
    }
//must also sign in the contractAddress
function encodeMessage(uint value, uint expiry, uint16[] ticketIndices)
    internal view returns (bytes32)
{
    bytes memory message = new bytes(84 + ticketIndices.length * 2);
    address contractAddress = getContractAddress();
    for (uint i = 0; i < 32; i++)
    {   // convert bytes32 to bytes[32]
        // this adds the price to the message
        message[i] = byte(bytes32(value << (8 * i)));
    }

    for (i = 0; i < 32; i++)
    {
        message[i + 32] = byte(bytes32(expiry << (8 * i)));
    }

    for(i = 0; i < 20; i++)
    {
        message[64 + i] = byte(bytes20(bytes20(contractAddress) << (8 * i)));
    }

    for (i = 0; i < ticketIndices.length; i++)
    {
        // convert int[] to bytes
        message[84 + i * 2 ] = byte(ticketIndices[i] >> 8);
        message[84 + i * 2 + 1] = byte(ticketIndices[i]);
    }

    return keccak256(message);
}

function name() public view returns(string)
{
    return name;
}

function symbol() public view returns(string)
{
    return symbol;
}

function getAmountTransferred() public view returns (uint)
{
    return numOfTransfers;
}

function balanceOf(address _owner) public view returns (bytes32[])
{
    return inventory[_owner];
}

function myBalance() public view returns(bytes32[]){
    return inventory[msg.sender];
}

function transfer(address _to, uint16[] ticketIndices) public
{
    for(uint i = 0; i < ticketIndices.length; i++)
    {
        uint index = uint(ticketIndices[i]);
        assert(inventory[msg.sender][index] != bytes32(0));
        //pushes each element with ordering
        inventory[_to].push(inventory[msg.sender][index]);
        delete inventory[msg.sender][index];
    }
    emit Transfer(_to, ticketIndices);
}

function transferFrom(address _from, address _to, uint16[] ticketIndices)
    organiserOnly public
{
    for(uint i = 0; i < ticketIndices.length; i++)
    {
        uint index = uint(ticketIndices[i]);
        assert(inventory[_from][index] != bytes32(0));
        //pushes each element with ordering
        inventory[_to].push(inventory[msg.sender][index]);
        delete inventory[_from][index];
    }

    emit TransferFrom(_from, _to, ticketIndices);
}

function endContract() public organiserOnly
{
    selfdestruct(organiser);
}

function isStormBirdContract() public pure returns (bool)
{
    return true;
}

function getContractAddress() public view returns(address)
{
    return this;
}

}
```

USER APP：AlphaWallet

The source code is about to open.
https://github.com/alpha-wallet

- AlphaWallet is one of the few encrypted wallets that support ERC875.
- AlphaWallet supports custom XML documents for full display of World Cup ticket content. Including ticket level, team, time, date, city, venue, etc.。 https://github.com/alpha-wallet/contracts/blob/master/FIFA%20WC2018/schema1/TicketingContract.sol

```
<attribute-type id="locality" oid="2.5.4.7" syntax="1.3.6.1.4.1.1466.115.121.1.15">
    <name lang="en">City</name>
    <name lang="zh">城市</name>
    <name lang="es">Ciudad</name>
    <name lang="ru">город</name>
    <origin as="mapping"
bitmask="00000000000000000000000000000000FF000000000000000000000000000000">
      <option key="1">
        <value lang="ru">Москвá</value>
        <value lang="en">Moscow</value>
        <value lang="zh">莫斯科</value>
        <value lang="es">Moscú</value>
      </option>
```

- AlphaWallet provides four different security level signatures for custom XML documents, ensuring security and customized

```
<ds:SignatureValue>
kporx19FbGkNJaJAF4hMmpT6riH/lv2wdJdoMOIj8JVva5KIBc4eY0TW3tGz6sH7QwtAkDtb+n92
41/ebewwRVGHqYQ6lsNiS1AXq14e3nnSQkBEB4IwJ/4svy57e2TqQsPgiYfyf0kNpvQnhIUbHX6z
zSg6McerMl4Tlo7sE/+gUw==
</ds:SignatureValue>
```

- Users can reach the Shankai Sports Ticketing in the AlphaWallet platform directly without jumping to other Apps or browsers. The World Cup ticket Token can be converted into a dynamic offline QR code to meet ticket checking need. (The QR Code Changes every 30 seconds; the client no need to be online all the time.)

ORGANIZER APP：Usher Mobile App

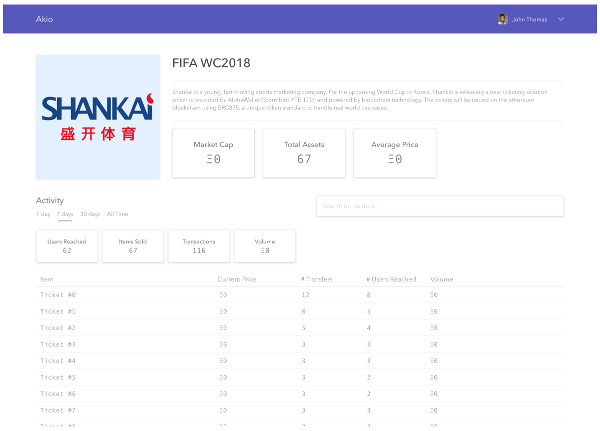
The source code is about to open
https://github.com/alpha-wallet

When checking the ticket, the Usher App is used to scan the QR code of the client, and the information on the blockchain and in the QR code are read for verification. When the scan passed, the user ticket (ERC875 Token) is destroyed to prevent reuse.

Data Managment

Akio is chose. It is the only available solution at present.
https://akiolabs.com/product/nft/

Akio is a data platform for Ethereum that provides insight into the activity of any smart contract. With it, you can transform the raw data, join it with other off-chain sources, or create charts to view core metrics that your stakeholders care about.


Akio John Thomas

FIFA WC2018

Shankai is a young, fast-moving sports marketing company. For the upcoming World Cup in Russia, Shankai is releasing a new ticketing solution which is provided by AlphaWallet (Stormbird PTE. LTD) and powered by blockchain technology. The tickets will be issued on the ethereum blockchain using ERC875, a unique token standard to handle real world use cases.

Market Cap Ξ0
Total Assets 67
Average Price Ξ0

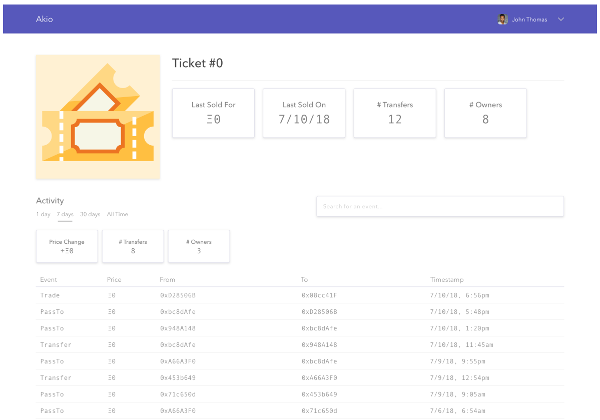
Activity
1 day 7 days 30 days All Time

Search for an item...

Users Reached 62
Items Sold 67
Transactions 116
Volume Ξ0

Item	Current Price	# Transfers	# Users Reached	Volume
Ticket #0	Ξ0	12	8	Ξ0
Ticket #1	Ξ0	6	5	Ξ0
Ticket #2	Ξ0	5	4	Ξ0
Ticket #3	Ξ0	3	3	Ξ0
Ticket #4	Ξ0	3	3	Ξ0
Ticket #5	Ξ0	3	2	Ξ0
Ticket #6	Ξ0	3	2	Ξ0
Ticket #7	Ξ0	3	3	Ξ0
Ticket #8	Ξ0	3	3	Ξ0

Fig.8 All ticket information within the Shankai contract


Akio John Thomas

Ticket #0

Last Sold For Ξ0
Last Sold On 7/10/18
Transfers 12
Owners 8

Activity
1 day 7 days 30 days All Time

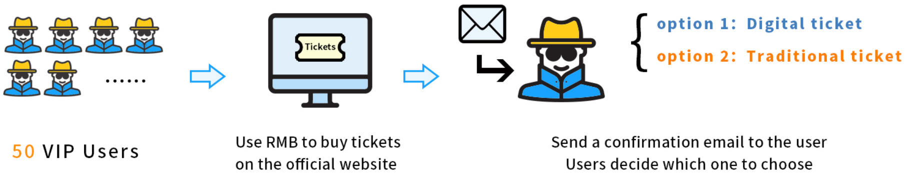
Search for an event...

Price Change +Ξ0
Transfers 8
Owners 3

Event	Price	From	To	Timestamp
Trade	Ξ0	0xD28506B	0x08cc41F	7/10/18, 6:56pm
PassTo	Ξ0	0xbc8dAfe	0xD28506B	7/10/18, 5:48pm
PassTo	Ξ0	0x948A148	0xbc8dAfe	7/10/18, 1:20pm
Transfer	Ξ0	0xbc8dAfe	0x948A148	7/10/18, 11:45am
PassTo	Ξ0	0xA66A3F0	0xbc8dAfe	7/9/18, 9:55pm
Transfer	Ξ0	0x453b649	0xA66A3F0	7/9/18, 12:54pm
PassTo	Ξ0	0x71c650d	0x453b649	7/9/18, 9:05am
PassTo	Ξ0	0xA66A3F0	0x71c650d	7/6/18, 6:54am

Fig.9 Resale information of single ticket

TEST CONTENT


option 1: Digital ticket
option 2: Traditional ticket
Tickets
50 VIP Users
Use RMB to buy tickets on the official website
Send a confirmation email to the user
Users decide which one to choose

In the test, we selected 50 opening ceremony VIP users. They used RMB to buy tickets on the official website, and received a confirmation email sent by the Shankai Sports. The email reminds them there are two options, digital ticketing solution or traditional way (ticket voucher), they can choose. The digital ticket contains a MagicLink and using instruction. Users are free to choose blockchain tickets and to import them into AlphaWallet. They just need to redeem the final paper ticket using AlphaWallet at the ticket exchange counter in Russia before the start of the opening.

RESULT

1. User acceptance of digital tickets

In the end, 28 people chose the blockchain ticket and successfully used the blockchain ticket to redeem the paper ticket. The conversion rate is higher than expected. We have reason to believe that if users can only use digital tickets, it will be widely accepted.

2. Is there any unforeseen problem during using AlphaWallet ? (for user)

In some countries, in order to protect consumers from digital currency fraud, a one-size-fits-all policy has been adopted that does not allow blockchain applications to be released.

3. Is there any unforeseen problems when using Usher Mobile App (for organizer)

Many users want left their blockchain tickets as souvenir instead of being destroyed. Finally, Shankai Sports agreed the 28 people kept their blockchain tickets. They keep additional record of these ticket’s information to prevent reuse.

4. Ethereum's impact on user experience（As shown in Table 3）

User Experience	Influences	
	For Users	For Shankai Sports
Importing Ticket	**Have a large influence** Tickets will only be shown after the transaction confirmed at Ethereum. When Ethereum congestion happened, Confirmation may be delayed by 14 hours.	**Have a certain influence** The user may continue to call Shankai Sports to confirm whether the ticket has been successfully imported.
Using Ticket	**Almost have no influence** Dynamic QR code can be used offline. The effect is limited to when the destroyed ticket disappears from the client.	**Almost have no effect** There may be a very small number of users trying to reuse the ticket before it disappeared, but it will not succeed.
Transfering Ticket	**Have a large influence** Tickets will only be shown after the transaction confirmed at Ethereum. When Ethereum congestion happened, Confirmation may be delayed by 14 hours.	**Have a certain influence** The user may continue to call Shankai Sports to confirm whether the ticket has been successfully transferred..
Selling Ticket	**Have a certain influence** Users need to learn what Ethereum is and how to trade before selling the blockchain ticket.	**Almost have no influence** Because both buyers and sellers have a certain understanding of Ethereum already.

Tabel 3 Ethereum's impact on user experience

AlphaWallet

Website https://www.awallet.io

Email info@awallet.io

Follow Us

- https://www.facebook.com/AlphaWallet/
- https://www.linkedin.com/company/awallet/
- https://twitter.com/Alpha_wallet
- https://www.reddit.com/r/AlphaWallet/
- https://github.com/alpha-wallet