

5 The most recent set of amended claims, filed on 11 January 2021, contains two independent claims which read as follows:

1. *A method of controlling a blockchain device activity by a controlling system comprising:*

a step of creating an at least one composite-key and a unique identification key, wherein an at least one control code is merged with the unique identification key to create the composite-key;

a step of creating a metadata describing the composite-key organization and the at least one control code organization;

a step of creating a redeem-script wherein the redeem-script comprising:

a step of hashing a input to the redeem-script;

a hash of the composite-key stored in the redeem-script;

a step of comparing hash of the input to the redeem-script and the hash of the composite-key stored in the redeem-script to give a comparison output;

a step of creating a blockchain address from the redeem-script comprising:

a step of creating a scriptPubKey by inserting the redeem-script hash into the scriptPubKey;

a step of encoding the scriptPubKey to create the blockchain address;

a step of sending a controlling-data through a communication system connected to the blockchain device through an at least one accessory;

wherein the controlling-data is defined as the set of control codes, the redeem-script, the metadata, the blockchain address, and the unique identification key;

the blockchain device is defined as a device connected to a blockchain and performing an at least one blockchain operation resulting in executing the blockchain device activity;

and the communication system is defined as a system connecting the controlling system to the blockchain device through an at least one accessory.

11. *A method of a blockchain device executing an at least one blockchain device activity, wherein the blockchain device is defined as a device connected to a blockchain for performing an at least one blockchain operation resulting in executing the blockchain device activity and the blockchain device is identified by an at least one unique identification key;*

the blockchain device using a controlling-data, wherein the controlling-data is defined as a set of control codes, a redeem-script, a metadata, a blockchain address, and the unique identification key;

wherein the redeem-script comprising:

a step of hashing a input to the redeem-script;

a hash of a composite-key stored in the redeem-script;

a step of comparing hash of the input to the redeem-script and the hash of the composite-key stored in the redeem-script to give a comparison output;

the blockchain device comprising:

a step of receiving the controlling-data from a communication system connected to an at least one accessory wherein the communication system is defined as a system connecting a controlling system to the blockchain device through the at least one accessory;

a step of processing the at least one control code, the unique identification key using the metadata to create a rebuilt-composite-key;

a step of creating a rebuilt redeem-script wherein the rebuilt redeem-script comprising:

a step of hashing a input to the rebuilt redeem-script;

a hash of the rebuilt-composite-key stored in the rebuilt redeem-script;

a step of comparing hash of the input to the rebuilt redeem-script and the hash of the rebuilt-composite-key stored in the rebuilt redeem-script to give a comparison output;

a step of creating a rebuilt blockchain address from the rebuilt redeem-script comprising:

a step of creating a scriptPubKey by inserting the rebuilt redeem-script hash into the scriptPubKey;

a step of encoding the scriptPubKey to create the rebuilt blockchain address;

a step of the blockchain device performing the at least one blockchain operation using the rebuilt-composite-key wherein the blockchain operation is selected from a group of blockchain operations the blockchain operation group consisting of:

verifying the correctness of the rebuilt-composite-key by checking the rebuilt blockchain address with the provided blockchain address from the accessory,

performs a blockchain transaction by spending a blockchain value in the blockchain address by processing the input to the rebuilt redeem-script using the rebuilt-composite-key,

verifies the at least one past blockchain transaction by checking the list of transactions for the blockchain address;

a step of the blockchain transaction resulting in a change in a state of the blockchain address;

a step of the blockchain transaction resulting in a change of the blockchain value in the blockchain address;

a step of triggering to execute the blockchain device activity by an at least one element in a list consisting of:

the blockchain value in the blockchain address,

the result of verifying the past blockchain transaction,

the result of verifying the correctness of the rebuilt blockchain address,

the result of the blockchain transaction performed,

the state of the blockchain address.

The Law

6 As I explained to Mr Ramesh at the hearing, I am bound to follow the law as it is set out in the Patents Act and related judgements of the UK courts.

7 The relevant portion of the Act is section 1(2) which sets out that certain things are excluded from patent protection. It says:

It is hereby declared that the following (among other things) are not inventions for the purposes of this Act, that is to say, anything which consists of -

a) ...;

b) ...;

c) a ... method for ... doing business, or a program for a computer;

d) ...;

but the foregoing provision shall prevent anything from being treated as an invention for the purposes of this Act only to the extent that a patent or application for a patent relates to that thing as such

8 The Court of Appeal in *Aerotel/Macrossan*¹ set out a four-step approach which assists in determining whether an invention is excluded.

(1) Properly construe the claim;

(2) Identify the actual contribution;

(3) Ask whether it falls solely within excluded subject matter;

(4) Check whether the actual or alleged contribution is actually technical in nature

9 In *Symbian*² the Court of Appeal reaffirmed the *Aerotel* approach while considering a question of “technical contribution” as it related to computer programs, emphasising the need to look at the practical reality of what the program achieved, and to ask whether there was something more than just a “better program”.

¹ *Aerotel Ltd v Telco Holdings Ltd & Ors* Rev 1 [2007] RPC 7

² *Symbian Ltd's Application* [2009] RPC 1

10 Subsequently *AT&T/Cvon*³ and *HTC v Apple*⁴ have provided us with five helpful signposts to apply when considering whether a computer program makes a relevant technical contribution. The signposts are:

i. whether the claimed technical effect has a technical effect on a process which is carried on outside the computer;

ii. whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run;

iii. whether the claimed technical effect results in the computer being made to operate in a new way;

iv. making the computer a better computer in the sense of running more efficiently and effectively as a computer;

v. whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

Analysis and arguments

Construing the claims

- 11 Mr Ramesh provided a detailed review of his invention at the hearing. He not only elaborated on the meaning of the terminology in his two independent claims, but he also explained the practical usefulness of his method with reference to a number of example applications. I am very grateful to Mr Ramesh for being so clear in his presentation.
- 12 It is perhaps worth briefly considering how the two independent claims are related. In simple terms claim 1 is directed towards creating a set of controlling data and sending that controlling data to a blockchain device. Claim 11 is about how the blockchain device makes use of that controlling data in order to execute an activity. To put it another way, the method of claim 1 generates the controlling data that is used in claim 11. The claims plainly go hand-in-hand and relate to one and the same invention. Whilst I acknowledge that claim 11 contains some additional subject matter relating to processes that may be carried out by the blockchain device, the claims will stand or fall together.
- 13 I need not comment on all the various steps in the claims in detail here. For the most part they are self explanatory. Mr Ramesh was quite open in admitting that the details of some of the method steps in his independent claims are actually standard in the art, and as such they do not present the skilled reader with any difficulties in understanding.
- 14 The step in the method which is of most interest is the one which appears to distinguish Mr Ramesh's method from the conventional methods, that is the step in which a composite key is created by merging a control code with a unique

³ *AT&T Knowledge Ventures/Cvon Innovations v Comptroller General of Patents* [2009] EWHC 343 (Pat)

⁴ *HTC v Apple* [2013] EWCA Civ 451

identification key. By way of example, the unique identification key could be a random number or string, and the control code could be a one-time-password.

- 15 It is not immediately apparent what sort of devices and device activities fall within the scope of the independent claims. The claims are cast quite broadly in this respect. Dependent claims 14 and 15 and the description provide some assistance. The applications of the method include, for example, performing financial transactions such as redeeming coupons, undertaking administrative actions such as signing documents, and GPS location-based unlocking of drones.
- 16 I note that the examiner has some reservations about the clarity of claim 11, but having had the benefit of Mr Ramesh's explanation at the hearing I am of the opinion that there are no significant clarity or claim construction issues upon which my decision on patentability would turn.

Identifying the contribution

- 17 Mr Ramesh and the examiner have not reached an agreement on what the contribution is.
- 18 The examiner's view is that the contribution of independent claim 1 is:

Using a blockchain transaction to perform an action (such as transferring money, signing documents, validating users' identities, financial transactions, issuing coupons, recording asset transferrals, billing, license management, gaming activities and unlocking drones) at a blockchain device by sending controlling data comprising control codes (a representation of an instruction to be performed by the device), a redeem script, a metadata, a blockchain address and a unique identification key from a controlling system to a blockchain device via an accessory, wherein: the redeem script stores a hash of a composite key created by merging one of the control codes with the unique identification key and comprises instructions to hash an input and compare the two hashes to give an output; the metadata describes how the composite key and control code are organised; and the blockchain address is created from the redeem script.

- 19 The examiner's contribution is quite closely related to the language of the claim. Mr Ramesh put it to me that this indicated that the examiner had not looked at his invention as a whole, or considered it in its proper context of the invention, or focussed on the central idea of the invention. I am not at all sure that is true, but in any case I have formed my own conclusion of the contribution, taking account of what the examiner says and what Mr Ramesh argued in the hearing.
- 20 Mr Ramesh has defined his contribution with reference to paragraph [0040] of his description, which reads:

[0040] Briefly, the following problems are not easily implementable using existing bitcoin standard-scripts usage mechanisms:

- Multi-user approvals, using traditional login/password or one-time passwords.
- Remote locking/unlocking devices through blockchain.

- Location-based triggering of activities through blockchain.
- Multi-user document signing, using traditional login, OTP.
- Easily redeemable coupons issued on the blockchain.

With that in mind he says that the contribution is:

a new blockchain device or an improved computer that can solve the problems cited in line [0040] of the specification

21 As I explained to Mr Ramesh at the hearing there is clearly something lacking from his version of the contribution. It is of course true that identifying the contribution should involve looking at the problem being solved, but it is necessary to do more than that. Paragraph 43 of *Aerotel* emphasises the factors that should be considered:

“How do you assess the contribution? Mr Birss submits the test is workable—it is an exercise in judgment probably involving the problem said to be solved, how the invention works, what its advantages are. What has the inventor really added to human knowledge perhaps best sums up the exercise.”

Mr Ramesh has, in my view, overlooked how the invention works and what its advantages are. As a result, his version of the contribution is simply too broad.

22 Before moving on to consider how the method works, I need to say a few words on what the problem actually is. One might be tempted to conclude, from Mr Ramesh’s alleged contribution viewed in the light of paragraph [0040], that the problem is how to enable multi-user approvals, remote locking/unlocking, location based triggering, multi user document signing and coupon redeeming via a blockchain. I do not doubt that the method provides a means by which such activities may be controlled using a blockchain, but Mr Ramesh acknowledged at the hearing that the known techniques already provide for such control. The problem is not that such things cannot be done using known custom-contracts or smart-contracts, but that the existing methods are not accepted in the industry. Paragraphs [0023]-[0024] of the description explains why – it is because they use non-standard Opcodes which are prone to the introduction of bugs. In fact, Mr Ramesh is correct to say that paragraph [0040] identifies the problem – it is that the list of activities is not easily implementable using existing bitcoin standard scripts.

23 So, in the context of that problem, how does Mr Ramesh’s method enable the control of devices connected to a blockchain without the use of non-standard Opcodes? Mr Ramesh explained this very clearly to me at the hearing with reference to each of the applications listed in paragraph [0040]. I do not need to go through each of his explanations in detail, but it is useful to look at a couple of examples.

24 In the case of multi-user approvals Mr Ramesh gave the example of two users, perhaps a husband and wife, who both have to sign a contract before a transaction can happen. Both have to provide an OTP (one time password). The OTP, in this example, forms part of the control code. The method joins the passwords together along with a unique ID key (which is unknown to the two users) to form a composite key. The composite key is then used, in the manner defined in the claims, to perform the transaction.

- 25 In the case of remote locking and unlocking Mr Ramesh explained that GPS information is stored in the control code. Again, the GPS data is joined with a unique ID key for form a composite key which is used, in the manner defined in the claims, to provide the GPS location to the blockchain device to enable location based locking and unlocking of the device, which may for instance be a drone.
- 26 It is quite clear to me that the key to how the method works is the composite key, if you will pardon the pun.
- 27 What then are the advantages of Mr Ramesh's method over known techniques? Having had the benefit of Mr Ramesh's insight into the state of the art I am content to accept that the advantage is that it does to succumb to the bugs which result from the use of non-standard opcodes.
- 28 With all that in mind I believe that the contribution, which is common to the two independent claims, can be summarised briefly as follows:

Using a composite key, which comprises control information merged with a unique identification key, within a blockchain to control activities of a blockchain device.

- 29 At the hearing I suggested to Mr Ramesh that I might find the actual contribution to be along these lines. I understood Mr Ramesh to be in agreement with such a contribution, having had the opportunity to discuss the details of his invention with me.

Does the contribution relate solely to excluded matter, or is technical?

- 30 There is no doubt that what Mr Ramesh has devised is a new computer program. Mr Ramesh does not argue otherwise. But a computer program can make a contribution outside the excluded fields. If the contribution is technical then the computer program is more than a computer program as such. The *AT&T* signposts are not a definitive test or a checklist, but they are a helpful way of assessing whether a computer program may give rise to such a technical contribution.
- 31 I can deal with signposts ii-iv quickly. Despite making some arguments in earlier correspondence, Mr Ramesh has not relied upon these signposts in his skeleton arguments or at the hearing, and I think that is quite correct. I can see nothing which points towards a technical effect at the level of the architecture of the computer, or a computer being made to operate in a new way, or an increase in reliability of speed of a computer. A computer when performing Mr Ramesh's method does not fundamentally change how it operates; it merely does something different by virtue of being programmed differently.
- 32 Mr Ramesh has argued that his method involves a technical effect on a process outside the computer and as such the first *AT&T* signpost is satisfied. His point is that his invention enables blockchain devices to carry out activities such as starting, stopping, locking and unlocking to be enabled on blockchain devices. Before looking at whether such activities might be considered a technical effect outside of a computer it is important to first note that there is nothing which limits the claims to the specific activities Mr Ramesh mentions.

- 33 In fact, it is quite clear that the claims are broad enough to cover a number of embodiments which relate to other activities, such as conducting financial transactions e.g. redeeming coupons, validating user identity e.g. by passwords, and administrative actions e.g. signing documents. These are the sorts of things that might well fall within the scope of the business method exclusion. I put this to Mr Ramesh at the hearing. He suggested to me that even these things involved something taking place outside of a computer. By way of example, he explained that his method allowed coupons to be printed. There is a brief reference to this in the description, which refers to the coupon controlling data being printed as a QR-code which may be scanned by a coupon encashing device. I do not see how this advances the argument. Even if this persuaded me that the activities I have mentioned above might involve some aspect which takes place outside of a computer (and I am not saying that I am persuaded) the first *AT&T* signpost requires more than this. It asks whether there is a technical effect on a process carried on outside of a computer. Mr Ramesh's invention, in my view, quite clearly embraces blockchain device activities which are non-technical in nature, and that is enough to conclude that the first signpost is not satisfied.
- 34 But what of the start/stop/lock/unlock activities that Mr Ramesh refers to? The specification describes these activities in the context of location-based triggering of drones. At first sight this may appear to point towards the possibility of there being a technical effect on a process which is carried on outside of a computer, but some careful consideration is necessary. It is important not to lose sight of the contribution, as I have defined it above. The contribution relates to the use of a composite key within a blockchain to control an activity of a blockchain device. Whilst the claimed method, in one embodiment, may result in the issuing of a command to a drone the contribution does not relate to any technical steps of controlling the drone per se. What has been contributed is a new way of using a blockchain to deliver control instructions to a device such as drone, and not a new way of controlling a device. The control instructions per se, and the activity that takes place when those instructions are executed, are entirely standard. I am therefore of the opinion that even in the embodiments of the invention which relate to remote locking/unlocking and location based triggering of activities of devices such as drones, the contribution does not involve a technical effect on a process carried on outside a computer.
- 35 Mr Ramesh considers that the fifth *AT&T* signpost is satisfied. His argument is a simple one - the problem is solved, not circumvented. I agree with Mr Ramesh to some extent. His method does indeed solve a problem, but as I have set out above the problem he has solved is that prior methods have not met with the approval of users because there is too much scope for the introduction of bugs in non-standard Opcodes. This problem is very clearly in the realm of computer programming; it is not a technical problem. As such I do not believe that the fifth signpost assists Mr Ramesh.
- 36 Having carefully considered all the points put before me at the hearing and in the skeleton arguments, and having reviewed the earlier correspondence on file, I am of the opinion that the contribution is not technical and falls squarely under the computer program exclusion for the reasons I have set out above. It is evident that the invention is a method of encoding control information in a blockchain. That information may be used to cause the performance of various activities, some of

which may even take place outside of a computer, but that does not change what the invention contributes as a matter of substance – it is a computer program as such.

- 37 Whilst the examiner also objected that the application relates to a business method it this not an issue that was addressed in any detail in the hearing, or indeed in Mr Ramesh's skeleton arguments. Having already determined that the claimed invention lies solely in the excluded field as a program for a computer as such I do not see the need to consider the business method objection.

Conclusion

- 38 I find that claims 1-20 are excluded from patent protection under section 1(2)(c) of the Act because they relate to a computer program as such. The application is therefore refused under section 18(3).

Appeal

- 39 Any appeal must be lodged within 28 days after the date of this decision.

J Pullen

Deputy Director, acting for the Comptroller